D-Link®

DSL-2640T
ADSL2+ Wireless Router
User Guide

August 2006

Table Of Contents

BEFORE YOU START 1
Installation Overview 1
Setup Wizard 1
Packing List 1
Installation Notes 2

INTRODUCTION 5
Router Description and Operation 5
Router Features 6
802.11g Wireless 7
Installation Considerations 8
Front Panel Display 9
Rear Panel Connections 10
Reset 11

HARDWARE INSTALLATION 12
Power on Router 12
Factory Reset Button 12
Network Connections 13

BASIC ROUTER CONFIGURATION 14
Computer IP Settings 14
Access the Configuration Manager 15
Login to Home Page 15
Configure the Router 16
Wizard 17
Wireless 27
Wireless Security 28
WAN 32
Bridge Mode 32
Dynamic IP Address 34
Static IP Address 37
PPPoE/PPPoA 40
LAN 46
DHCP 47
DNS 50
Dynamic DNS 51
Save Settings and Reboot 52
Multiple Virtual Connections 53

ADVANCED MANAGEMENT 55
UPnP 56

Virtual Server **57**
LAN Clients **60**
SNMP 61
Filters **62**
Bridge Filters 64
Static Routing 65
DMZ 66
Parental Control **67**
URL Blocking 68
Domain Blocking 68
Firewall **69**
RIP 70
PPP 71
ADSL 72
ATM VCC 73
QOS **74**
Wireless Management **80**
Access List 80
Associated Stations 81
Multiple SSID 82
Wireless Distribution System 83
Wireless Performance 85

TOOLS **87**
Change System Password **88**
Remote Web Management and Remote Telnet Access 89
Time **90**
Remote Log 91
Save or Load Configuration File 92
Restore Factory Default Settings **92**
Firmware Upgrade **93**
Miscellaneous Configuration 94
Ping Test 94
IGMP Proxy 94
Diagnostic Test **95**

STATUS **96**
Device Info **96**
DHCP Clients 97
Log 98
Statistics 99
ADSL Status 100
Help 101

TECHNICAL SPECIFICATIONS **102**

CONFIGURING IP SETTINGS ON YOUR COMPUTER **105**

LOW PASS FILTERS FOR DSL **111**

About This User Guide

This user's guide provides instructions on how to install the DSL-2640T ADSL 2+ Router and use it to provide Internet access for an Ethernet network or single computer.

If you are using a computer with a functioning Ethernet port, the quickest and easiest way to set up the DSL-2640T is to follow the instructions provided in the **Quick Installation Guide**.

Before You Start

Please read and make sure you understand all the prerequisites for proper installation of your new Router. Have all the necessary information and equipment on hand before beginning the installation.

Installation Overview

The procedure to install the Router can be described in general terms in the following steps:

1. Gather information and equipment needed to install the device. Before you begin the actual installation make sure you have all the necessary information and equipment.
2. Install the hardware, connect the cables to the device, and connect the power adapter.
3. Check the IP settings on your computer and change them if necessary so the computer can access the web-based software built into the Router.
4. Use the web-based management software to configure the device to suit the requirements of your ADSL service and requirements of your local network.

Setup Wizard

Many users will be able to configure all the settings necessary to use the DSL-2640T with the Setup Wizard. For ADSL connections that use PPPoE or PPPoA connections, the simplest way to set up the DSL-2640T is to use the Setup Wizard to configure the Internet connection. Once you access the web interface used to configure the device, just launch the Setup Wizard to configure your Internet connection.

Packing List

Open the shipping carton and carefully remove all items. Make sure that you have the items listed here.

- One DSL-2640T ADSL Ethernet Router
- One CD-ROM containing the User's Guide and Quick Installation Guide
- One twisted-pair telephone cable used for ADSL connection
- One straight-through Ethernet cable
- One AC power adapter suitable for your electric service
- One Quick Installation Guide

Installation Notes

In order to establish a connection to the Internet it will be necessary to provide information to the Router that will be stored in its memory. For some users, only their account information (Username and Password) is required. For others, various parameters that control and define the Internet connection will be required. You can print out the two pages below and use the tables to list this information. This way you have a hard copy of all the information needed to setup the Router. If it is necessary to reconfigure the device, all the necessary information can be easily accessed. Be sure to keep this information safe and private.

Low Pass Filters

Since ADSL and telephone services share the same copper wiring to carry their respective signals, a filtering mechanism may be necessary to avoid mutual interference. A low pass filter device can be installed for each telephone that shares the line with the ADSL line. These filters are easy to install passive devices that connect to the ADSL device and/or telephone using standard telephone cable. Ask your service provider for more information about the use of low pass filters with your installation.

Operating Systems

The DSL-2640T uses an HTML-based web interface for setup and management. The web configuration manager may be accessed using any operating system capable of running web browser software, including Windows 98 SE, Windows ME, Windows 2000, and Windows XP.

Web Browser

Any common web browser can be used to configure the Router using the web configuration management software. The program is designed to work best with more recently released browsers such as Microsoft Internet Explorer® version 6.0, Netscape Navigator® version 6.2.3, or later versions. The web browser must have JavaScript enabled. JavaScript is enabled by default on many browsers. Make sure JavaScript has not been disabled by other software (such as virus protection or web user security packages) that may be running on your computer.

Ethernet Port (NIC Adapter)

Any computer that uses the Router must be able to connect to it through the Ethernet port on the Router. The easiest method of installation is via the Ethernet connection and therefore requires that your computer be equipped with an Ethernet port as well. Most notebook computers are now sold with an Ethernet port already installed. Likewise, most fully assembled desktop computers come with an Ethernet NIC adapter as standard equipment. If your computer does not have an Ethernet port, you must install an Ethernet NIC adapter before you can use the Router. If you must install an adapter, follow the installation instructions that come with the Ethernet NIC adapter.

Additional Software

For a bridged connection, the information needed to make and maintain the Internet connection is stored on another computer or gateway device using PPP client or similar third party client software, not in the Router itself.

If your ADSL service is delivered through a PPPoE, PPPoA or Static IP connection, the information needed to establish and maintain the Internet connection can be stored in the Router. In this case, it is not necessary to install software on your computer. It may however be necessary to change some settings in the device, including account information used to identify and verify the connection.

Information you will need from your ADSL service provider:

Username	This is the Username used to log on to your ADSL service provider's network. It is commonly in the form – user@isp.co.uk Your ADSL service provider uses this to identify your account.	Record info here
Password	This is the Password used, in conjunction with the Username above, to log on to your ADSL service provider's network. This is used to verify the identity of your account.	
WAN Setting / Connection Type	These settings describe the method your ADSL service provider uses to transport data between the Internet and your computer. Most users will use the default settings. You may need to specify one of the following WAN Setting and Connection Type configurations (Connection Type settings listed in parenthesis): PPPoE/PPoA (PPPoE LLC, PPPoA LLC or PPPoA VC-Mux) Bridge Mode (1483 Bridged IP LLC or 1483 Bridged IP VC-Mux) Static IP Address (Bridged IP LLC, 1483 Bridged IP VC-Mux, 1483 Routed IP LLC, 1483 Routed IP VC-Mux or IPoA) Dynamic IP Address (1483 Bridged IP LLC or 1483 Bridged IP VC-Mux) Default = PPPoE/PPPoA (PPPoE LLC)	
VPI	Most users will not be required to change this setting. The Virtual Path Identifier (VPI) is used in conjunction with the Virtual Channel Identifier (VCI) to identify the data path between your ADSL service provider's network and your computer. If you are setting up the Router for multiple virtual connections, you will need to configure the VPI and VCI as instructed by your ADSL service provider for the additional connections. This setting can be changed in the WAN Settings window of the web management interface. Default value = 8	
VCI	Most users will not be required to change this setting. The Virtual Channel Identifier (VCI) used in conjunction with the VPI to identify the data path between your ADSL service provider's network and your computer. If you are setting up the Router for multiple virtual connections, you will need to configure the VPI and VCI as instructed by your ADSL service provider for the additional connections. This setting can be changed in the WAN Settings window of the web management interface. Default value = 35	

Note

The Setup Wizard can be used to configure the Internet connection for most users.

Information you will need about your DSL-2640T ADSL 2+ Router:

Username	This is the Username needed access the Router's management interface. When you attempt to connect to the device through a web browser you will be prompted to enter this Username. The default Username for the Router is "admin." The user cannot change this.	Record info here
Password	This is the Password you will be prompted to enter when you access the Router's management interface. The default Password is "admin." The user may change this.	
LAN IP addresses for the DSL-2640T	This is the IP address you will enter into the Address field of your web browser to access the Router's configuration graphical user interface (GUI) using a web browser. The default IP address is **192.168.1.1**. This may be changed to suit any IP address scheme the user desires. This address will be the base IP address used for DHCP service on the LAN when DHCP is enabled.	
LAN Subnet Mask for the DSL-2640T	This is the subnet mask used by the DSL-2640T, and will be used throughout your LAN. The default subnet mask is **255.255.255.0**. This can be changed later.	

Information you will need about your LAN or computer:

Ethernet NIC	If your computer has an Ethernet NIC, you can connect the DSL-2640T to this Ethernet port using an Ethernet cable. You can also use the Ethernet ports on the DSL-2640T to connect to other computer or Ethernet devices.	Record info here
DHCP Client status	Your DSL-2640T ADSL 2+ Router is configured, by default, to be a DHCP server. This means that it can assign an IP address, subnet mask, and a default gateway address to computers on your LAN. The default range of IP addresses the DSL-2640T will assign are from **192.168.1.2** to **192.168.1.254**. Your computer (or computers) needs to be configured to **Obtain an IP address automatically** (that is, they need to be configured as DHCP clients.)	

It is recommended that your collect and record this information here, or in some other secure place, in case you have to re-configure your ADSL connection in the future.

Once you have the above information, you are ready to setup and configure your DSL-2640T ADSL 2+ Router.

1

Introduction

This section provides a brief description of the Router, its associated technologies, and a list of Router features.

Router Description and Operation

The DSL-2640T Wireless ADSL2+ Router is designed to provide connectivity for your private Ethernet LAN, and 802.11g/802.11b wireless LAN to the Internet via an ADSL connection.

The Router is easy to install and use. Standard Ethernet ports are used to connect to computer or other Ethernet devices. The 802.11g wireless interface provides connectivity to 802.11g or 802.11b wireless devices.

802.11g Wireless

The embedded 802.11g wireless access point provides Internet access and connectivity to the Ethernet for 802.11g and 802.11b wireless workstations. IEEE 802.11g is fully compatible with IEEE 802.11b wireless devices. The 802.11g standard supports data transfer rates of up to 54 Mbps. The wireless Router supports 64-bit and 128-bit WEP encryption.

ADSL

Asymmetric Digital Subscriber Line (ADSL) is a broadband network technology that utilizes standard twisted-pair copper wire telephone lines to enable broadband high-speed digital data transmission and bandwidth hungry applications for business and residential customers.

ADSL2+ routers and modems provide faster downloads and more reliable connectivity to the user without loss of quality or disruption of voice/fax telephone capabilities.

ADSL2+ provides a dedicated service over a single telephone line operating at speeds of up to 24Mbps downstream and up to 1Mbps upstream, depending on local telephone line conditions. A secure point-to-point connection is established between the user and the central office of the service provider.

D-Link ADSL devices incorporate the recommendations of the ADSL Forum regarding framing, data format, and upper layer protocols.

Router Features

The DSL-2640T ADSL 2+ Router utilizes the latest ADSL enhancements to provide a reliable Internet portal suitable for most small to medium sized offices. DSL-2640T advantages include:

- **PPP (Point-to-Point Protocol) Security –** The DSL-2640T ADSL 2+ Router supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol) for PPP connections.
- **DHCP Support –** Dynamic Host Configuration Protocol automatically and dynamically assigns all LAN IP settings to each host on your network. This eliminates the need to reconfigure every host whenever changes in network topology occur.
- **Network Address Translation (NAT) –** For small office environments, the DSL-2640T allows multiple users on the LAN to access the Internet concurrently through a single Internet account. This provides Internet access to everyone in the office for the price of a single user.

  NAT improves network security in effect by hiding the private network behind one global and visible IP address. NAT address mapping can also be used to link two IP domains via a LAN-to-LAN connection.
- **TCP/IP (Transfer Control Protocol/Internet Protocol) –** The DSL-2640T supports TCP/IP protocol, the language used for the Internet. It is compatible with access servers manufactured by major vendors.
- **RIP-1/RIP-2 –** The DSL-2640T supports both RIP-1 and RIP-2 exchanges with other routers. Using both versions lets the Router to communicate with all RIP enabled devices.
- **Static Routing –** This allows you to select a data path to a particular network destination that will remain in the routing table and never "age out". If you wish to define a specific route that will always be used for data traffic from your LAN to a specific destination within your LAN (for example to another router or a server) or outside your network (to an ISP defined default gateway for instance).
- **Default Routing –** This allows you to choose a default path for incoming data packets for which the destination address is unknown. This is particularly useful when/if the Router functions as the sole connection to the Internet.
- **ATM (Asynchronous Transfer Mode) –** The DSL-2640T supports Bridged Ethernet over ATM (RFC1483), IP over ATM (RFC1577) and PPP over ATM (RFC 2364).
- **Precise ATM Traffic Shaping –** Traffic shaping is a method of controlling the flow rate of ATM data cells. This function helps to establish the Quality of Service for ATM data transfer.
- **G.hs (Auto-handshake) –** This allows the Router to automatically choose either the G.lite or G.dmt ADSL connection standards.
- **High Performance –** Very high rates of data transfer are possible with the Router. Up to 8 Mbps downstream bit rate using the G.dmt standard.
- **Full Network Management –** The DSL-2640T incorporates SNMP (Simple Network Management Protocol) support for web-based management and text-based network management via an RS-232 or Telnet connection.
- **Telnet Connection –** The Telnet enables a network manager to access the Router's management software remotely.
- **Easy Installation –** The DSL-2640T uses a web-based graphical user interface program for convenient management access and easy set up. Any common web browser software can be used to manage the Router.

802.11g Wireless

In order to get the best performance from the wireless component of the Router, you should have some basic understanding of how wireless networks operate. There are more factors to consider when setting up or designing a wireless network than designing a wired network. If you are setting up a wireless network, especially if you are using multiple access points and/or covering a large area, good planning from the outset can ensure the best possible reliability, performance, coverage and effective security.

Radio Transmission

Wireless local network (also called WI-FI) devices such as notebook computers and wireless access points use electromagnetic waves within a broad, unlicensed range of the radio spectrum (between 2.4GHz and 2.5GHz) to transmit and receive radio signals. A wireless access point (AP) becomes a base station for the wireless nodes (a notebook computer for example) in its broadcast range. Often a wireless access point such as the AP embedded in the DSL-2640Twill also provide a connection to a wired network - usually Ethernet - and ultimately an Internet connection. The IEEE 802.11 standard precisely defines the encoding techniques used for data transmission. The DSL-2640Tcan be used by IEEE 802.11g and 802.11b devices. These two standards are compatible but use different encoding methods for data transmission.

802.11g uses a method called Orthogonal Frequency Division Multiplexing (OFDM) for transmitting data at higher data rates. OFDM is a more efficient encoding method than Direct Sequence Spread Spectrum (DSSS) transmission, the method used by 802.11b devices. However, in order to support different data transmission rates while maintaining compatibility with 802.11b - 802.11g uses a combination of OFDM and DSSS when 802.11b devices are present.

Range

An access point will send and receive signals within a limited range. The actual effective range of the AP can vary depending on operating conditions. Radio signals are emitted in all directions giving the access point a spherical range. The physical environment in which the AP is operating can impact on its effectiveness and range. If you experience low signal strength or slow throughput, consider positioning the Router in a different location. See Installation Considerations below concerning the wireless environment and location of the AP (DSL-2640T).

SSID

Wireless networks use an SSID (Service Set Identifier) as means of identifying a group of wireless devices, similar to a domain or subnet. This allows wireless devices to roam from one AP to another and remain connected. Wireless devices that wish to communicate with each other must use the same SSID. Several access points can be set up using the same SSID so that wireless stations can move from one location to another without losing connection to the wireless network.

The embedded wireless access point of the Router operates in *Infrastructure* mode. It controls network access on the wireless interface in its broadcast area. It will allow access to the wireless network to devices using the correct SSID after a negotiation process takes place. By default, the DSL-2640Tbroadcasts its SSID so that any wireless station in range can learn the SSID and ask permission to associate with it. Many wireless adapters are able to survey or scan the wireless environment for access points. An access point in Infrastructure mode allows wireless devices to survey that network and select an access point with which to associate. You may disable SSID broadcasting in the web manager's wireless menu.

Channel

The AP can operate on different channels (frequency bands). This is useful when multiple APs are used in order to avoid unwanted overlap or interference between control zones of separate APs. Wireless nodes must use the same SSID and the same channel as the AP with which it will associate. However, using the same channel on two different APs can contribute wireless congestion under certain circumstances. If you are using multiple APs on your network and are experiencing low throughput or significant transmission delay, carefully consider how channels are assigned to the different APs.

Wireless Security

Various security options are available on the Router including open or WEP and WPA.

Installation Considerations

Many physical environmental factors can impact wireless networks. Radio waves are used to carry the encoded data between devices. These radio transmissions can become degraded due to signal attenuation, multi-path distortion and interference or noise. Attenuation simply means that the strength of the signal weakens with the distance it travels, even if the transmission path is unobstructed. Multi-path distortion occurs when radio signals bounce off objects like walls, ceilings, metal appliances, etc. This may cause a signal to be duplicated, with each separate yet identical signal arriving at a receiver at different times. Interference and noise from electrical devices such as microwave ovens, fluorescent lights, automobile engines and other radio emitting devices can cause signal degradation. With all of this in mind, choose a location for all your access points including the DSL-2640T.

The access point can be placed on a shelf or desktop, ideally you should be able to see the LED indicators on the front if you need to view them for troubleshooting.

Wireless networking lets you access your network from nearly anywhere you want. However, the number of walls, ceilings, or other objects that the wireless signals must pass through can limit signal range. Typical ranges vary depending on the types of materials and background RF noise in your home or business. To range and signal strength, use these basic guidelines:

Keep the number of walls and ceilings between the DSL-2640Tand other network devices to a minimum - each wall or ceiling can reduce your D-Link wireless product’s range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.

Be aware of the direct line between network devices. A wall that is 1.5 feet thick (.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.

Materials can impede the wireless signal - a solid metal door or aluminum studs may have a negative effect on range. Try to position wireless devices and computers with wireless adapters so that the signal passes through drywall or open doorways and not dense, especially metallic, materials. Also, note that metal filing cabinets and appliances can reflect radio signals. When these metal objects are moved around, your wireless network may be affected.

Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate extreme RF noise such as microwave ovens, CRT monitors, motors, etc.

Front Panel Display

Place the Router in a location that permits an easy view of the LED indicators on the front panel.

The LED indicators on the front panel include **Power**, **Status**, **ADSL** and **Ethernet**. The **ADSL**, and **Ethernet** indicators monitor link status and activity (**Link/Act**).

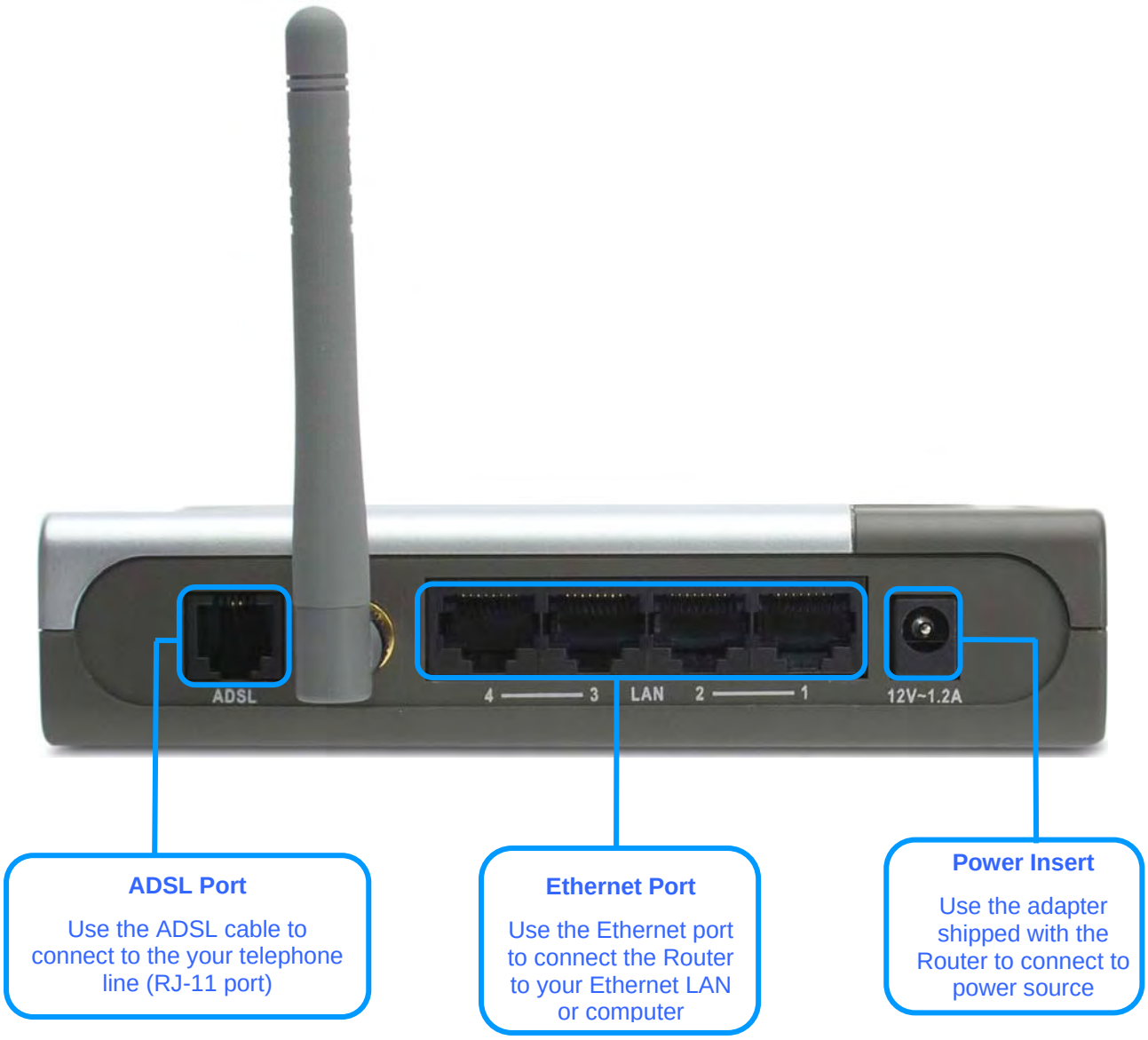
Power	Steady green light indicates the unit is powered on. When the device is powered off this remains dark.
Status	Lights steady green during power on self-test (POST). Once the connection status has been settled, the light will blink green. If the indicator lights steady green after the POST, the system has failed and the device should be rebooted.
ADSL (Link/Act)	Steady green light indicates a valid ADSL connection. This will light after the ADSL negotiation process has been settled. A blinking green light indicates activity on the WAN (ADSL) interface.
WLAN (Link/Act)	Steady green light indicates a wireless connection. A blinking green light indicates activity on the WLAN interface.
LAN 1-4 (Link/Act)	A solid green light indicates a valid link on startup. This light will blink when there is activity currently on any Ethernet port.

Rear Panel Connections

All cable connections to the Router are made at the rear panel. Connect the power adapter here to power on the Router. Use the Reset button to restore the settings to the factory default values in the next chapter for instructions on using the reset button).

Connect network cables:

1. Insert the ADSL (telephone) cable included with the Router into the ADSL port and then connect the cable to your telephone line.
2. Insert one end of the Ethernet cable into the Ethernet (LAN) port on the back panel of the Router and the other end of the cable to an Ethernet Adapter or available Ethernet port on your computer.


ADSL
4
3
LAN
2
1
12V~1.2A
ADSL Port
Use the ADSL cable to connect to the your telephone line (RJ-11 port)
Ethernet Port
Use the Ethernet port to connect the Router to your Ethernet LAN or computer
Power Insert
Use the adapter shipped with the Router to connect to power source

Reset

To Reset the Router to factory default settings including the default IP address 192.168.1.1, depress the reset button on the right side panel with a ballpoint pen, paper clip or similar object for a few seconds. The device will restart with default settings.

2

Hardware Installation

The DSL-2640T maintains two separate physical interfaces, an ADSL and an Ethernet interface. Place the Router in a location where it can be connected to the various devices as well as to a power source. The Router should not be located where it will be exposed to moisture or excessive heat. Make sure the cables and power cord are placed safely out of the way so they do not create a tripping hazard. As with any electrical appliance, observe common sense safety procedures.

The Router can be placed on a shelf or desktop, ideally you should be able to see the LED indicators on the front if you need to view them for troubleshooting.

Power on Router

CAUTION: The Router must be used with the power adapter included with the device.

To power on the Router:

1. Insert the AC Power Adapter cord into the power receptacle located on the rear panel of the Router and plug the adapter into a suitable nearby power source.
2. You should see the Power LED indicator light up and remain lit. The Status LED should light solid green and begin to blink after a few seconds.
3. If the Ethernet port is connected to a working device, check the Ethernet Link/Act LED indicators to make sure the connection is valid. The Router will attempt to establish the ADSL connection, if the ADSL line is connected and the Router is properly configured this should light up after several seconds. If this is the first time installing the device, some settings may need to be changed before the Router can establish a connection.

Factory Reset Button

The Router may be reset to the original factory default settings by depressing the reset button on the right side panel (see illustration on page 11) for a few seconds while the device is powered on. Use a ballpoint or paperclip to gently push down the reset button. Remember that this will wipe out any settings stored in flash memory including user account information and LAN IP settings. The device settings will be restored to the factory default IP address 192.168.1.1 and the subnet mask is 255.255.255.0, the default management Username is “admin” and the default Password is “admin.”

Network Connections

Network connections are provided through the ADSL port and Ethernet port on the back of the Router. See the Rear Panel diagram above and the illustrations below for examples.

Connect ADSL Line

Use the ADSL cable included with the Router to connect it to a telephone wall socket or receptacle. Plug one end of the cable into the ADSL port (RJ-11 receptacle) on the rear panel of the Router and insert the other end into the RJ-11 wall socket. If you are using a low pass filter device, follow the instructions included with the device or given to you by your service provider. The ADSL connection represents the WAN interface, the connection to the Internet. It is the physical link to the service provider's network backbone and ultimately to the Internet.

Connect Router to Ethernet

The Router may be connected to a single computer or Ethernet device through the 10/100 BASE-TX Ethernet port on the rear panel. Any connection to an Ethernet concentrating device such as a switch or hub must operate at a speed of 10/100 Mbps only. When connecting the Router to any Ethernet device that is capable of operating at speeds between 0~100Mbps, be sure that the device has auto-negotiation (NWay) enabled for the connecting port.

Use Category 5 or better twisted-pair Ethernet cable with RJ-45 connectors. The RJ-45 port on the Router is auto MDI-X/MDI-II meaning that is will link correctly with either MDI-II through or MDI-X crossed ports.

The rules governing Ethernet cable lengths apply to the LAN to Router connection. Be sure that the cable connecting the LAN to the Router does not exceed 100 meters.

3

Basic Router Configuration

The first time you setup the Router it is recommended that you configure the WAN connection using a single computer connected directly to the Router. Once the WAN connection is functioning properly, you may continue to make changes to Router configuration including IP settings and DHCP setup. For information on how to configure advanced features such as port redirection, filtering and firewall, please skip ahead to the Advanced Router Management section on page 55.

Configuration Summary

1. **Connect to the Router** To configure various settings used by the Router for Internet and access it is first necessary to access the Router's management HTML-based interface. This is done using an ordinary web browser. Your computer must be able to "see" the Router before it can manage it using a browser. If the Router is in the same "neighborhood" or subnet as the Router, you should be able to access the management software. Therefore you must first make sure your computer has IP settings that place it in the same subnet as the Router. The easiest way to make sure your computer has the correct IP settings is to configure it to use the DHCP server in the Router. The DHCP server will automatically enable your computer to use a browser to manage the Router. The next section describes how to change the IP configuration for a computer running a Windows operating system to be a DHCP client. If you are running another operating system, make sure your computer is configured as a DHCP client so it can automatically obtain IP settings from the Router. Some operating systems will automatically select the best IP settings. Consult the user manual for the operating system (OS) if you are unsure.

2. **Configure the Internet (WAN) Connection** Most users will be able to complete this process using the **Setup Wizard**. The Setup Wizard can be launched once you have successfully connected with the Router's management software. There are different methods used to establish the WAN connection to the service provider's network and ultimately to the Internet. Your Router may already have most of the settings configured by default. However you will probably at least have to type in a user name and password given to you by your ISP. You may also need to know the encapsulation and connection type required to use for your ADSL service. Your service provider should provide all the information needed to configure the WAN connection.

Computer IP Settings

In order to configure your system to receive IP settings from the Router your computer must first have the TCP/IP protocol installed. If you have an Ethernet port on your computer, it probably already has TCP/IP protocol installed. If you are using Windows XP the TCP/IP is enabled by default for standard installations. Instructions for configuring your computer to receive IP settings from the Router are provided in Appendix B on page 105.

For computers running non-Windows operating systems, follow the instructions for your OS that configure the system to receive an IP address from the Router, that is, configure the system to be a DHCP client.

Note

If you are not sure how to configure your Windows computer to be a DHCP client, see Configuring IP Settings on Your Computer begiining on page 105.

Access the Configuration Manager

In order to make sure your computer's IP settings allow it to communicate with the Router, it is advisable to configure your system be a DHCP client – that is, it will get IP settings from the Router. Appendix B describes how to configure different Windows operating systems to "Obtain IP settings automatically".

Note

Be sure that the web browser on your computer is not configured to use a proxy server in the Internet settings. In Windows Internet Explorer, you can check if a proxy server is enabled using the following procedure:

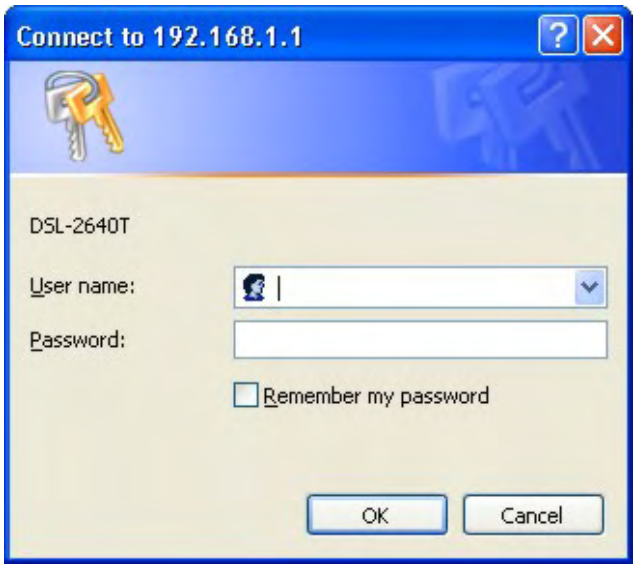
1. In Windows, click on the **Start** button and choose **Control Panel**.
2. In the **Control Panel** window, click on the **Network and Internet Options** icon.
3. In the **Network and Internet Connections** window, click the **Internet Options** icon.
4. In the **Internet Properties** window, click on the **Connections** tab and click on the **LAN Settings** button
5. Verify that the "Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections)." option is NOT checked. If it is checked, click in the checked box to deselect the option and click **OK**.

*Alternatively, you can access this **Internet Options** menu using the **Tools** pull-down menu in Internet Explorer.*

Login to Home Page

To use the web-based management software, launch a suitable web browser and direct it to the IP address of the Router. Type in **http://** followed by the default IP address, **192.168.1.1** in the address bar of the browser. The URL in the address bar should read: **http://192.168.1.1**.

A dialog box prompts for the User Name and Password. Type in the default User Name "admin," and the default Password "admin" then click the **OK** button to access the web-based manager.



Enter Password

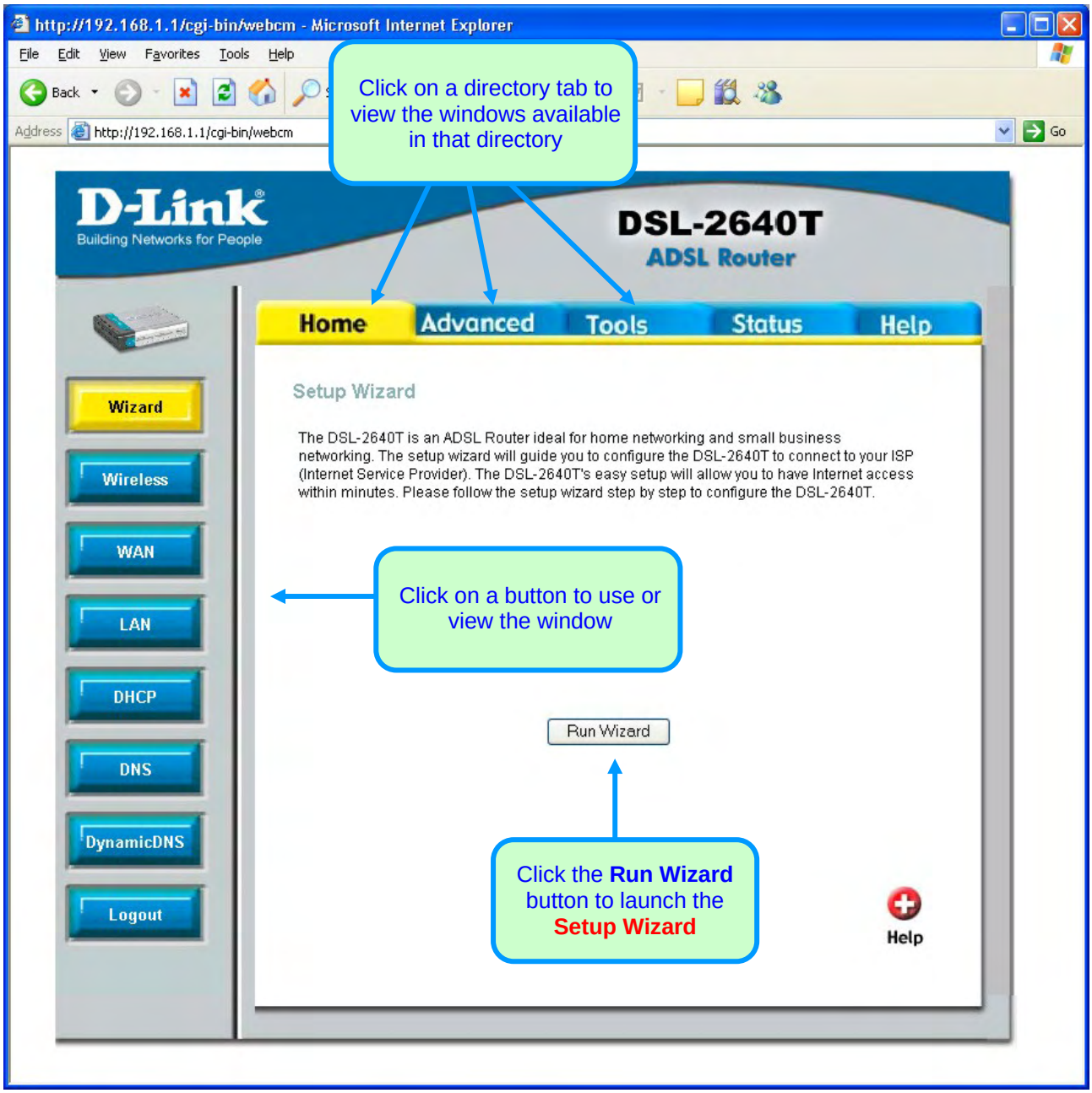
You should change the web-based manager access user name and password once you have verified that a connection can be established. The user name and password allows any PC within the same subnet as the Router to access the web-based manger.

Note

The user name and password used to access the web-based manager is NOT the same as the ADSL account user name and password needed for PPPoE/PPPoA connections to access the Internet.

Configure the Router

When you successfully connect to the web manager, the **Home** directory tab will display the **Setup Wizard** window. You can launch the Setup Wizard from this page or use the buttons located in the left panel of the web page to view other windows used for basic configuration.


http://192.168.1.1/cgi-bin/webcm - Microsoft Internet Explorer
Click on a directory tab to view the windows available in that directory
D-Link
Building Networks for People
DSL-2640T
ADSL Router
Home
Advanced
Tools
Status
Help
Wizard
Wireless
WAN
LAN
DHCP
DNS
DynamicDNS
Logout
Setup Wizard
The DSL-2640T is an ADSL Router ideal for home networking and small business networking. The setup wizard will guide you to configure the DSL-2640T to connect to your ISP (Internet Service Provider). The DSL-2640T's easy setup will allow you to have Internet access within minutes. Please follow the setup wizard step by step to configure the DSL-2640T.
Click on a button to use or view the window
Run Wizard
Click the Run Wizard button to launch the Setup Wizard
Help

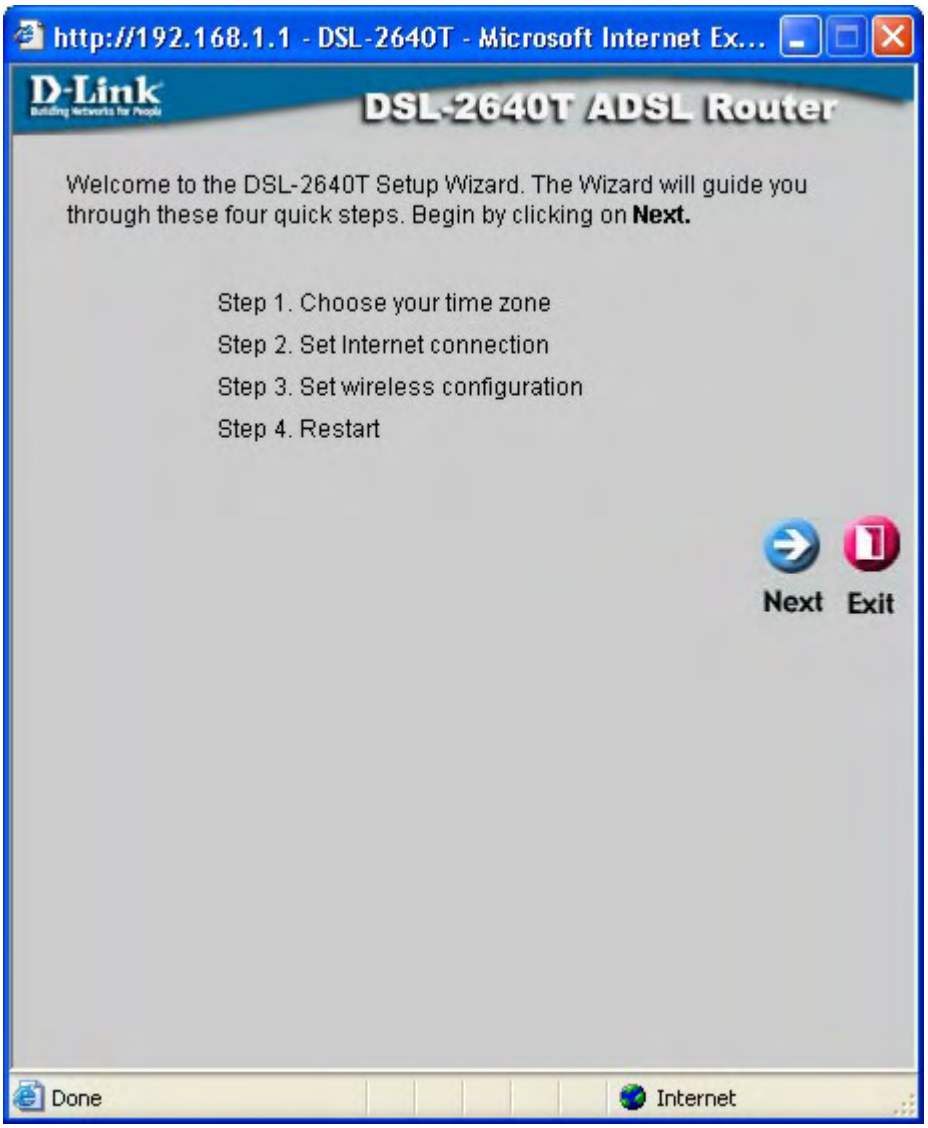
Web Manager – First Time Log On

All configuration and management of the Router is done using the web-based management interface pictured in the above example. The configuration windows are accessed by clicking on the directory tabs: **Home**, **Advanced**, **Tools**, **Status**, and **Help**. Each tab has associated window buttons in the left hand panel of the web interface. Basic setup of the Router can be completed in the windows accessed from the **Home** directory including: (Setup) **Wizard**, **WAN** (Internet), **LAN** (to configure the IP address of the Router) **DHCP**, **DNS** and **Dynamic DNS**.

Wizard

To use the Setup Wizard, click the **Run Wizard** button in the first browser window and follow the instructions in the pop-up window that appears.

The initial window summarizes the setup process. Click the **Next** button to proceed. You may stop using the Setup Wizard at any time by clicking the **Exit** button. If you exit the wizard you will return to the **Setup Wizard** window without saving any of the settings changed during the process.

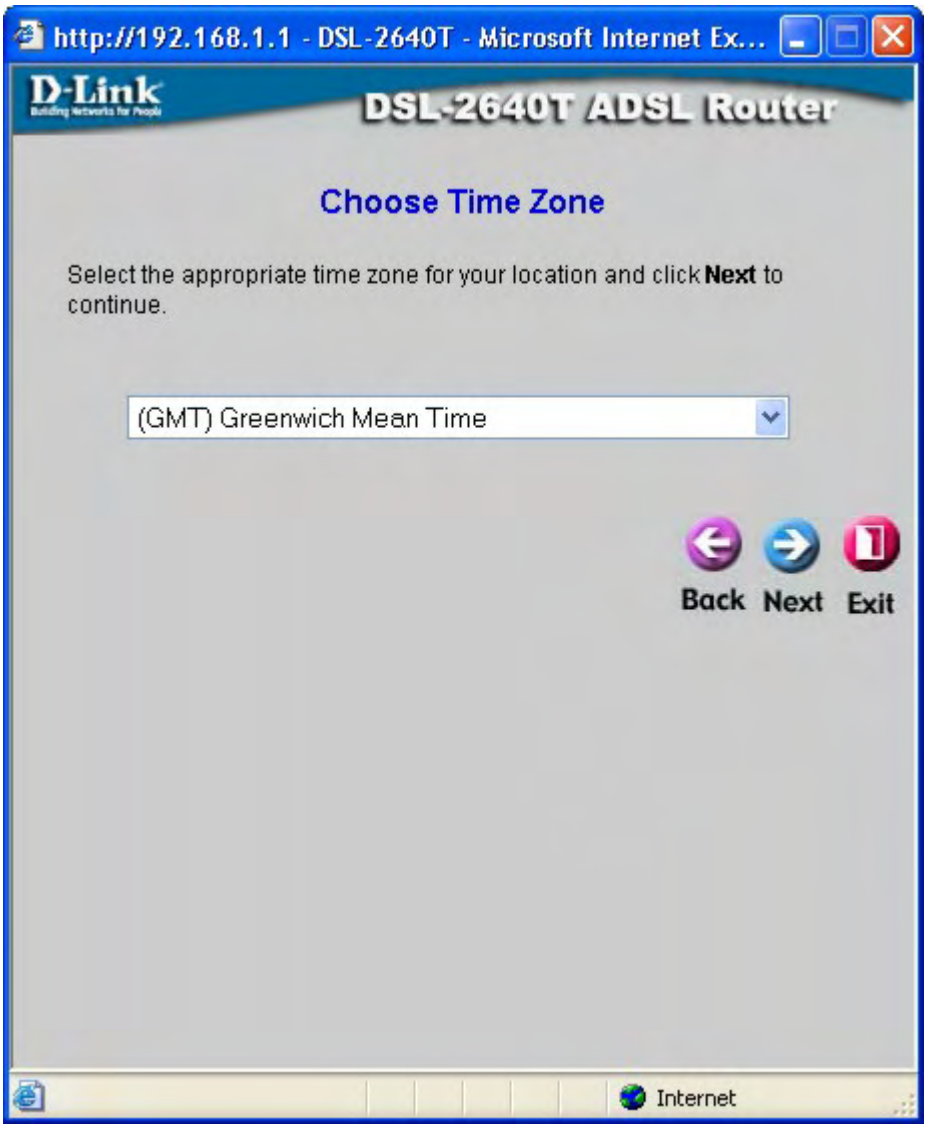

http://192.168.1.1 - DSL-2640T - Microsoft Internet Ex...
D-Link
DSL-2640T ADSL Router
Welcome to the DSL-2640T Setup Wizard. The Wizard will guide you through these four quick steps. Begin by clicking on Next.
Step 1. Choose your time zone
Step 2. Set Internet connection
Step 3. Set wireless configuration
Step 4. Restart
Next
Exit
Done
Internet

The first pop-up window of the Setup Wizard lists the basic steps in the process. These steps are as follows:

1. Set the system time.
2. Configure the connection to the Internet.
3. Save the new configuration settings and reboot the system.

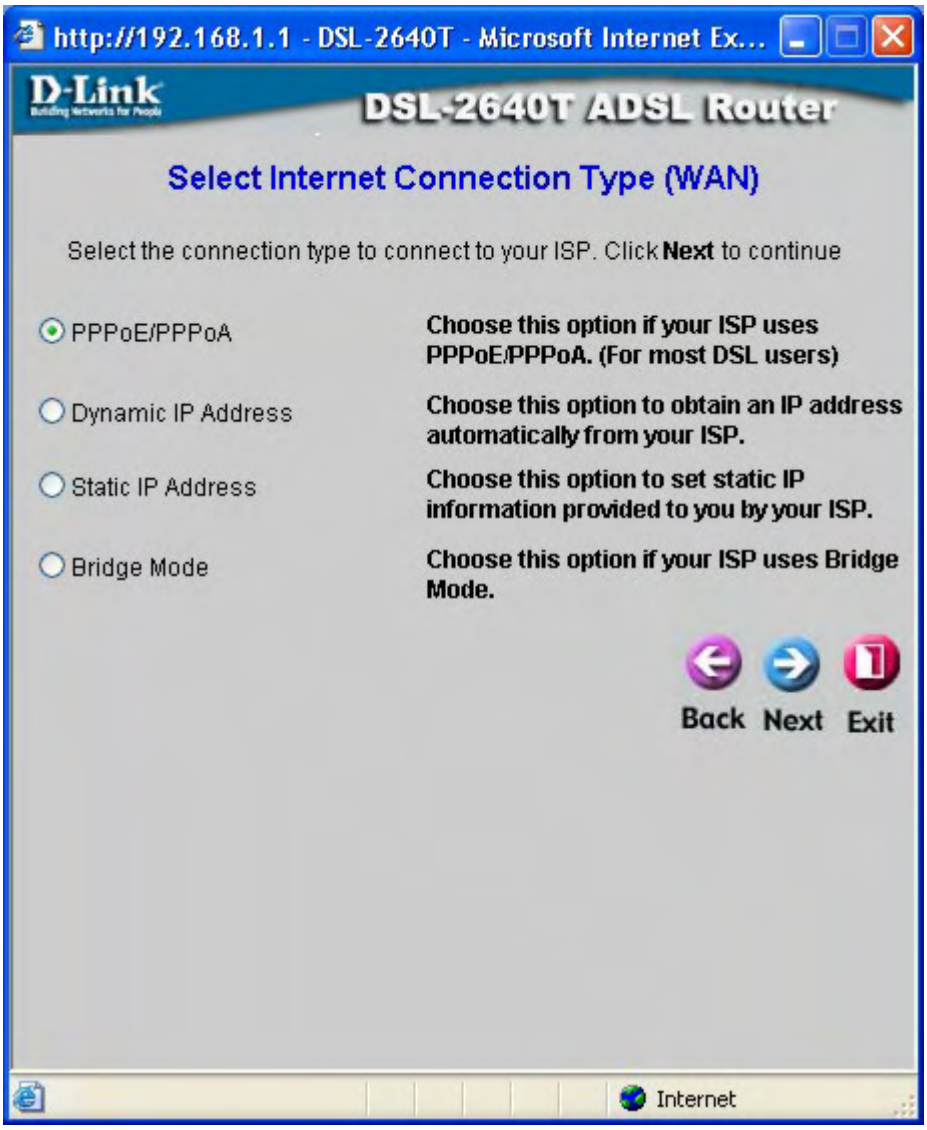
Using the Setup Wizard - Choose Time Zone

Choose the time zone you are in from the pull-down menu and click **Next**. This sets the system time used for the Router. If you wish to return to the previous window during the setup process, click the **Back** button.



Using the Setup Wizard - Choose Connection Type

Now select the Connection Type used for the Internet connection. Your ISP has given this information to you. The connection types available for "Multi-User" Mode are **PPPoE/PPPoA**, **Dynamic IP Address**, **Static IP Address**, and **Bridge Mode**. Each connection type has different settings that are configured in the next Setup Wizard pop-up window.


http://192.168.1.1 - DSL-2640T - Microsoft Internet Ex...
D-Link
DSL-2640T ADSL Router
Select Internet Connection Type (WAN)
Select the connection type to connect to your ISP. Click Next to continue
PPPoE/PPPoA
Choose this option if your ISP uses PPPoE/PPPoA. (For most DSL users)
Dynamic IP Address
Choose this option to obtain an IP address automatically from your ISP.
Static IP Address
Choose this option to set static IP information provided to you by your ISP.
Bridge Mode
Choose this option if your ISP uses Bridge Mode.
Back
Next
Exit
Internet

Select the **Connection Type** specific to your service and click **Next** to go to the next Setup Wizard pop-up window. Follow the instructions below for the type of connection you have selected.

Using the Setup Wizard - For PPPoE/PPPoA connections:

1. Type in the **Username** and **Password** used to identify and verify your account to the ISP.
2. Select the specific **Connection Type** from the drop-down menu. The available PPP connection and encapsulation types are *PPPoE LLC*, *PPPoA LLC* and *PPPoA VC-Mux*.
3. If you are instructed to change the **VPI** or **VCI** number, type in the correct setting in the available entry fields. Most users will not need to change these settings. The Internet connection cannot function if these values are incorrect.
4. Click **Next** to go to the next window and complete the Setup Wizard.

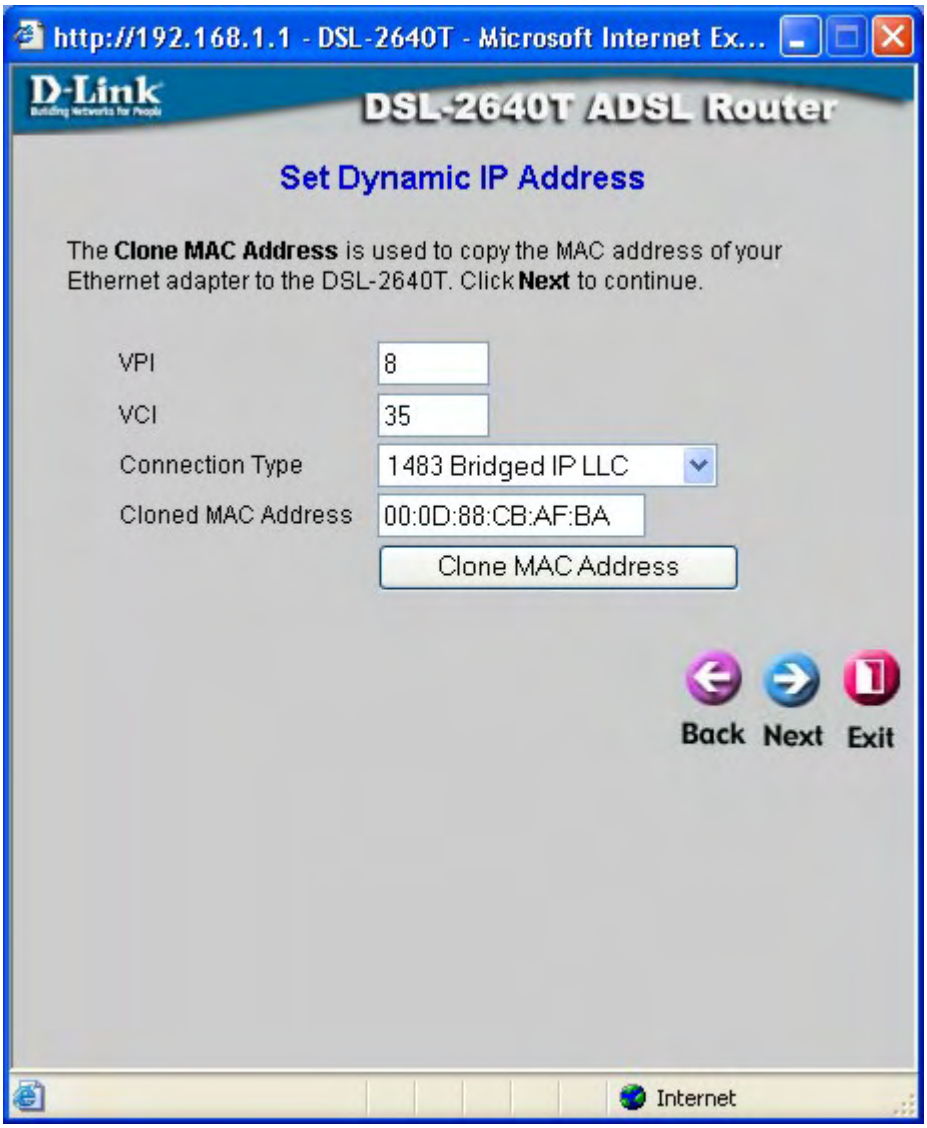
Using the Setup Wizard - For Dynamic IP Address connections:

1. Select the specific **Connection Type** from the drop-down menu. The available Dynamic IP Address connection and encapsulation types are *1483 Bridged IP LLC* and *1483 Bridged IP VC-Mux*.

2. If you are instructed to change the **VPI** or **VCI** number, type in the correct setting in the available entry fields. Most users will not need to change these settings. The Internet connection cannot function if these values are incorrect.

3. You may want to copy the MAC address of your Ethernet adapter to the Router. Some ISPs record the unique MAC address of your computer's Ethernet adapter when you first access their network. This can prevent the Router (which has a different MAC address) from being allowed access to the ISPs network (and the Internet). To clone the MAC address of your computer's Ethernet adapter, type in the MAC address in the Cloned MAC Address field and click the **Clone MAC Address** button. This will copy the information to a file used by the Router to present to the ISP's server used for DHCP.

4. Click **Next** to go to the next pop-up window and complete the Setup Wizard.



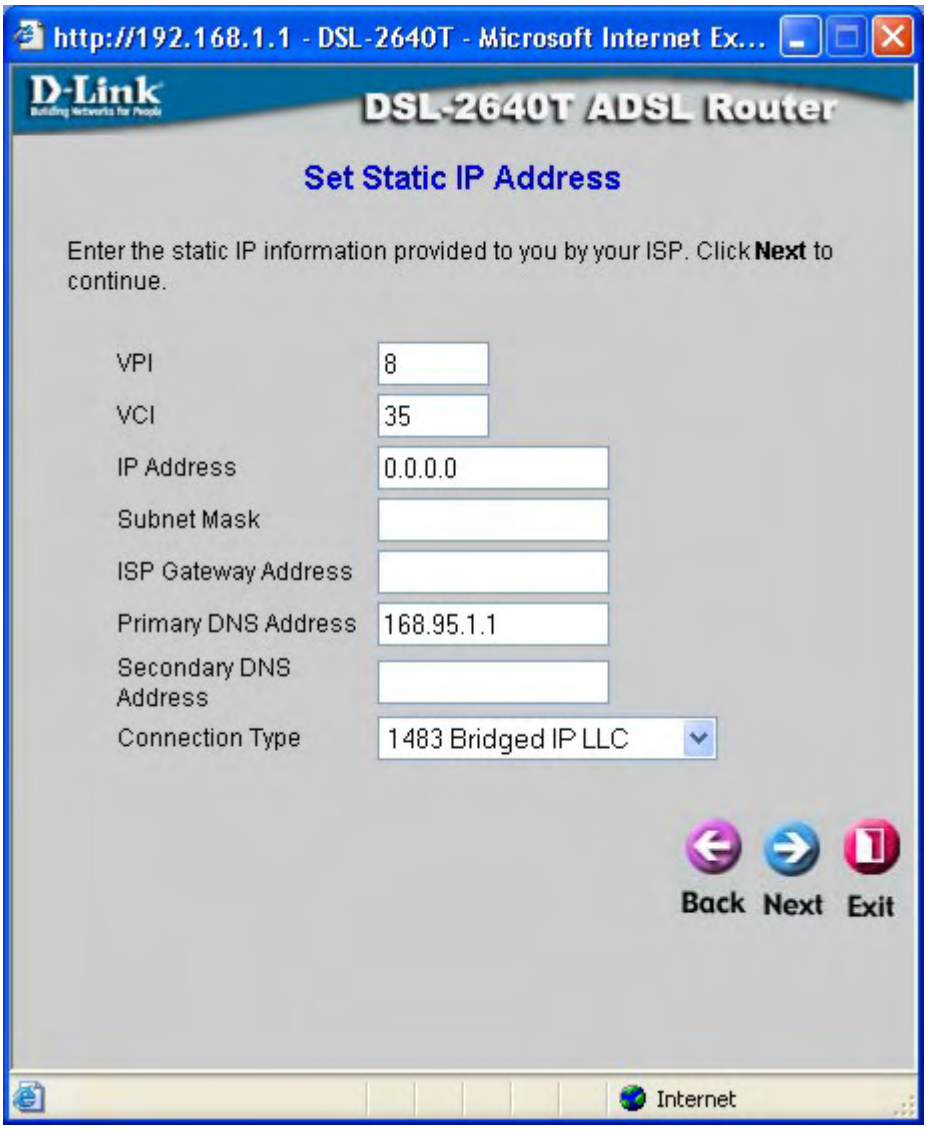
Using the Setup Wizard - For Static IP Address connections:

1. Select the specific **Connection Type** from the drop-down menu. The available Static IP Address connection and encapsulation types are *1483 Bridged IP LLC*, *1483 Bridged IP VC-Mux*, *1483 Routed IP LLC*, *1483 Routed IP VC-Mux* and *IPoA*.

2. Change the **IP Address**, **Subnet Mask**, **ISP Gateway Address**, **Primary DNS Address**, and **Secondary DNS** Server IP **Address** as instructed by your ISP. For IPoA connections it may also be necessary to change the **ARP Server Address**. IPoA connection users who have not been given this information should leave the field blank.

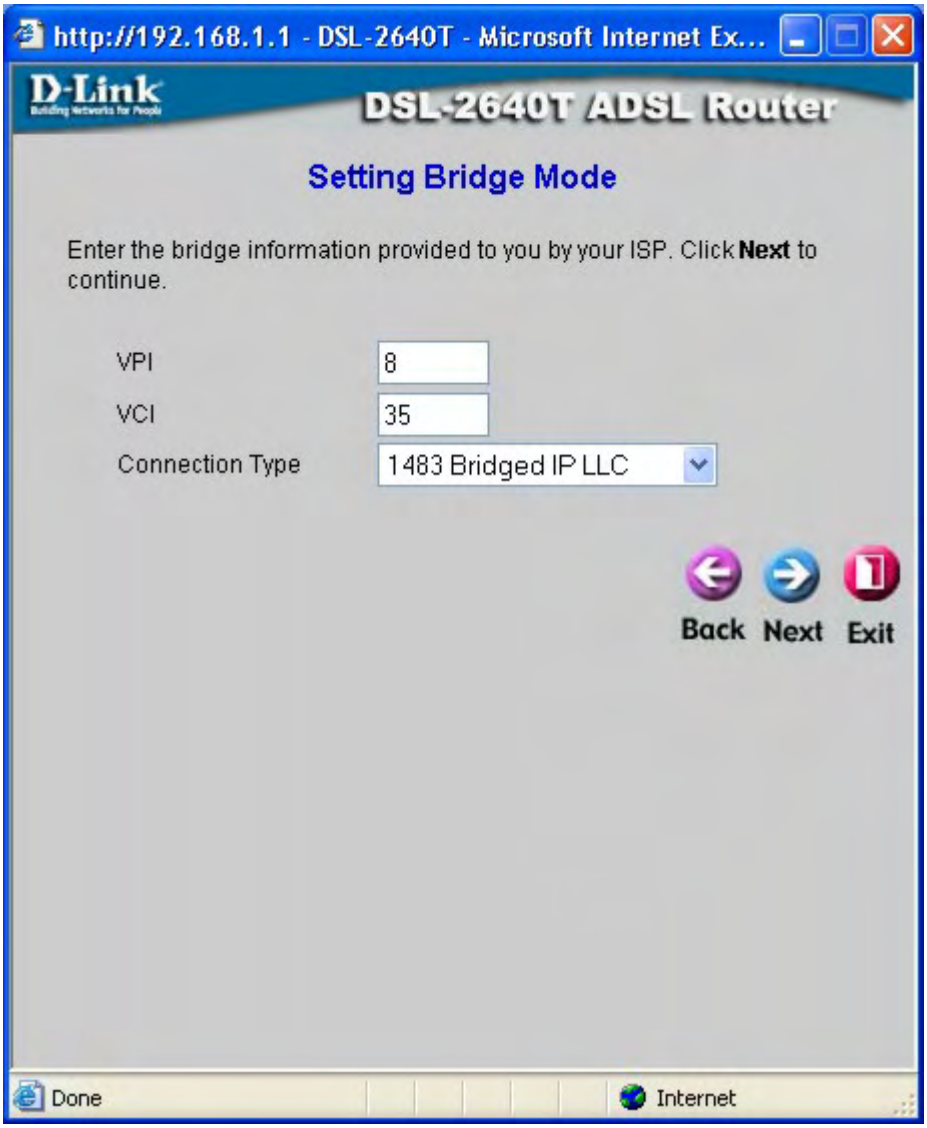
3. If you are instructed to change the **VPI** or **VCI** number, type in the correct setting in the available entry fields. Most users will not need to change these settings. The Internet connection cannot function if these values are incorrect.

4. Click **Next** to go to the next window and complete the Setup Wizard.



Using the Setup Wizard - For Bridge Mode connections:

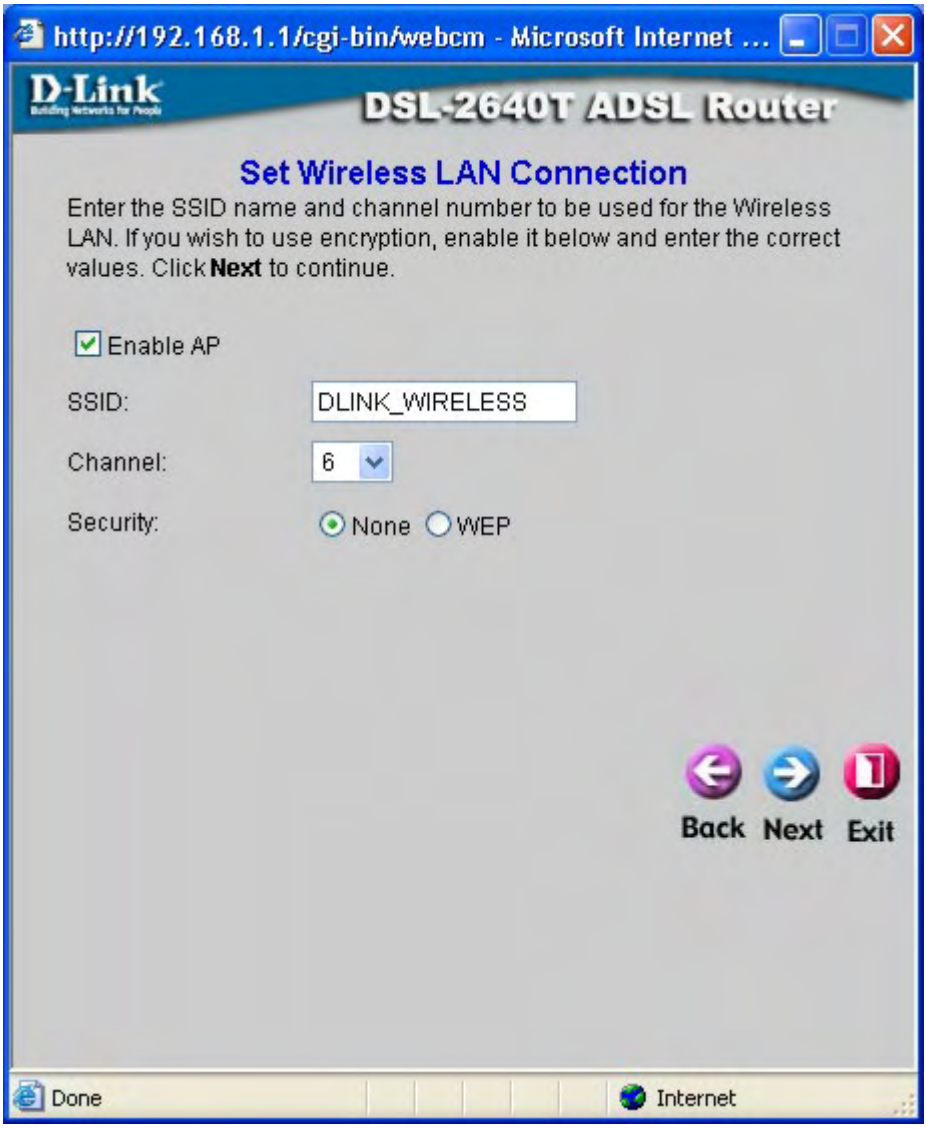
1. Select the specific **Connection Type** from the drop-down menu. The available Bridge Mode connection and encapsulation types are *1483 Bridged IP LLC* and *1483 Bridged IP VC-Mux*.
2. If you are instructed to change the **VPI** or **VCI** number, type in the correct setting in the available entry fields. Most users will not need to change these settings. The Internet connection cannot function if these values are incorrect.
3. Click **Next** to go to the next window and complete the Setup Wizard.



Using the Setup Wizard - Wireless LAN Configuration

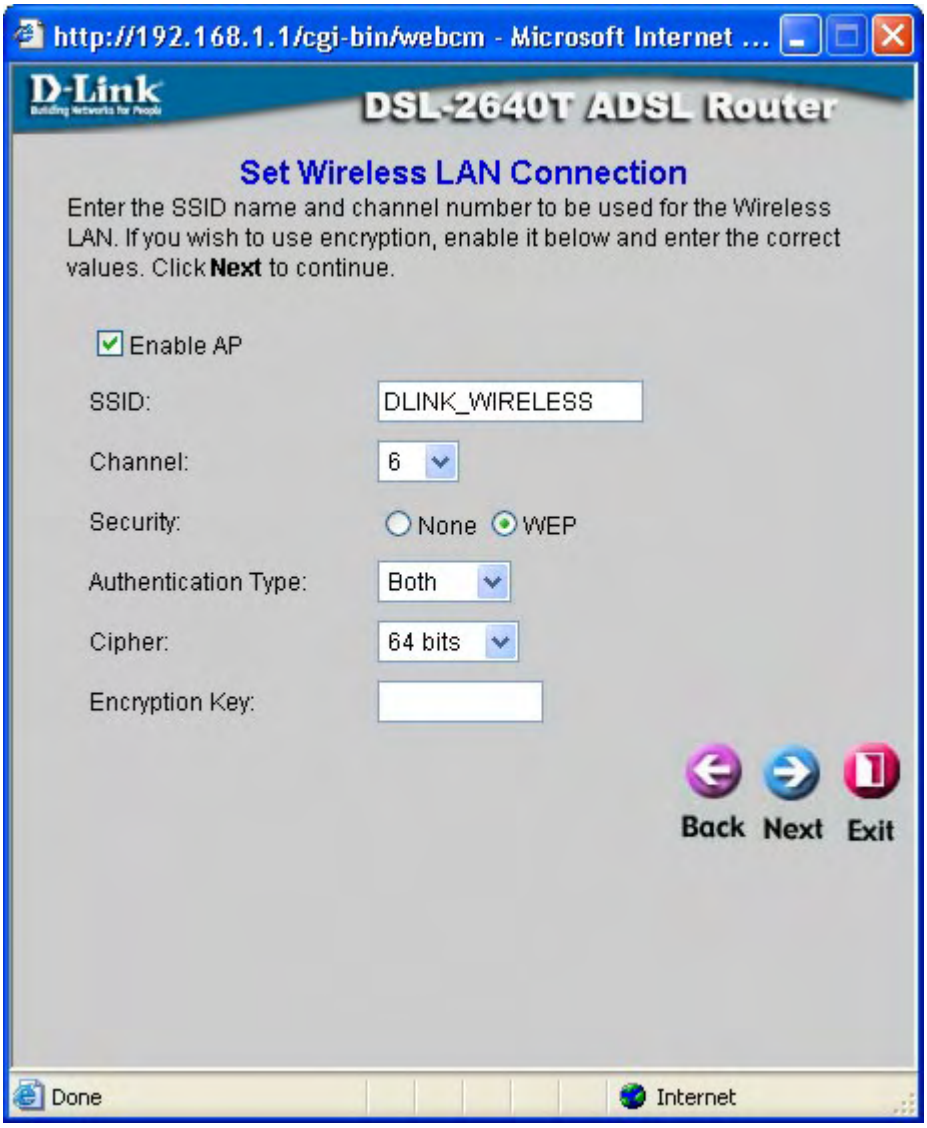
Configure the **SSID** and **Channel** for the Wireless LAN. You may also configure **WEP** security settings at this time or configure them later using the web manager. Select **None** to configure WEP later. To disable the wireless access point, click the **Enable AP** option box to remove the green check mark. To configure Wirless LAN settings:

1. Enter the **SSID** for the Wireless LAN
2. Choose the wireless **Channel** to be used for your WLAN from the pull down menu.
3. Choose the wireless security setup. If **WEP** is used an additional step is required for configuration
4. Click **Next**



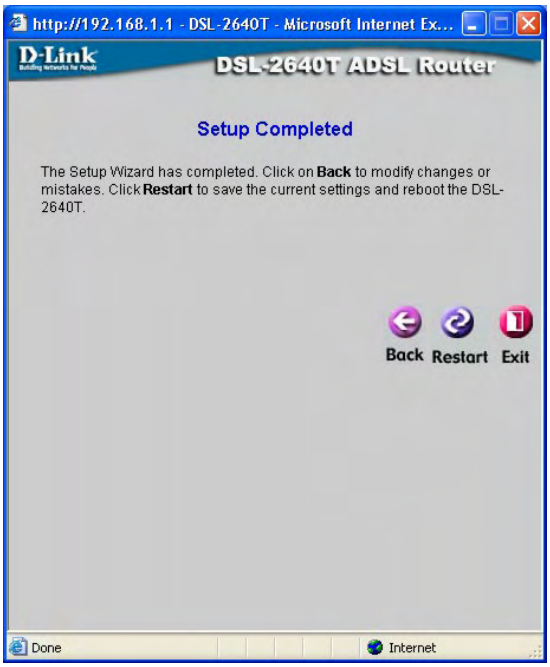
Using the Setup Wizard - WEP Configuration

If you are configuring WEP security, select the **Authentication Type**, **Cipher** rate and **Encryption Key**. Click **Next** to continue to the final menu.



Using the Setup Wizard - Finish and Restart

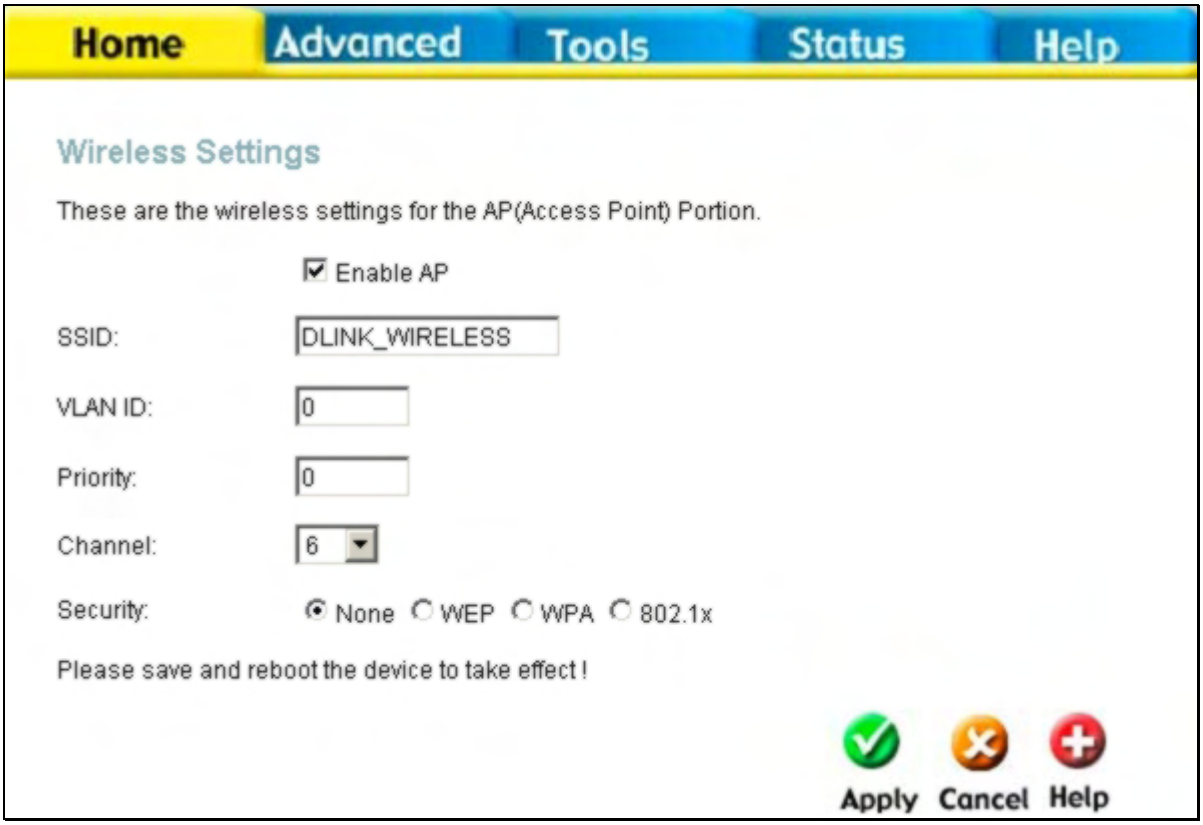
Finally you can confirm that the setup process is completed. If you are satisfied that you have entered all the necessary information correctly, click the **Restart** button to save the new configuration settings and restart the Router. If you need to change settings from a previous window, click the **Back** button.


http://192.168.1.1 - DSL-2640T - Microsoft Internet Ex...
D-Link
DSL-2640T ADSL Router
Setup Completed
The Setup Wizard has completed. Click on Back to modify changes or mistakes. Click Restart to save the current settings and reboot the DSL-2640T.
Back
Restart
Exit
Done
Internet

Do not turn the Router off while it is restarting. After the Router is finished restarting, you are now ready to continue to configure the Router as desired. You may want to test the WAN connection by accessing the Internet with your browser.

Wireless

To configure the Router's basic configuration settings without running the Setup Wizard, you can access the windows used to configure Wireless, WAN, LAN, DHCP, DNS, and Dynamic DNS settings directly from the **Home** directory. To access the **Wireless Settings** window, click on the **Wireless** link button on the left side of the first window that appears when you successfully access the web manager.



Wireless Settings menu – No Security

For Basic Wireless LAN operation with no Securtiy settings, follow the steps:

1. Click the **Enable AP** box to allow the router to operate in the wireless environment.
2. The **SSID** identifies members of the Service Set. Accept the default name or change it to something else. If the default SSID is changed, all other devices on the wireless network must use the same SSID.
3. What channels are available for use by the access point depends on the local regulatory environment. Remember that all devices communicating with the device must use the same channel (and use the same SSID). Use the drop-down menu to select the **Channel** used for your 802.11g wireless LAN. The wireless channel number is available from your Internet Service Provider (ISP).
4. The VLAN ID and Priority settings are optional settings. If your network supports VLANs or QoS Priority (IEEE 802.11p), type in the appropriate values here.
5. If network **Security** is not used, click to select **None**, then click **Apply**.

Note

VLAN ID and Priority settings do not need to be configured in order to use the Wireless Access Point.

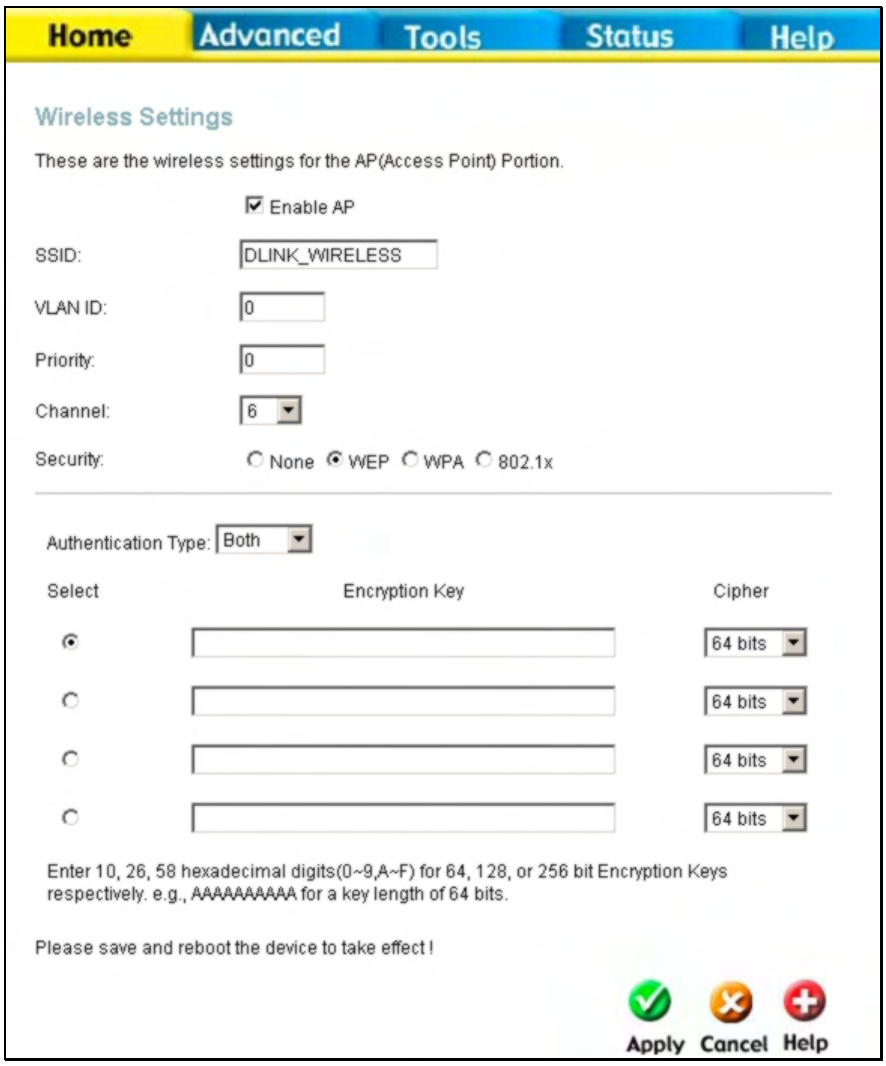
Wireless Security

In the **Wireless Settings** window, select the type of security you want to configure. The window will change to present the settings specific to the method being configured. The Router's wireless security options include three levels of WEP encryption, WPA for IEEE 802.1x network authentication, and WPA with a user-configured Pre Shared Key (PSK).

WEP

WEP (Wireless Encryption Protocol) encryption can be enabled for security and privacy. WEP encrypts the data portion of each frame transmitted from the wireless adapter using one of the predefined keys. The router offers 64-, 128-, or 256-bit encryption with four keys available.

To bring up the **Wireless Settings** window for WEP, click the **WEP** radio button.



Wireless Settings menu – WEP

1. Make sure the **Enable AP** checkbox at the top of the window has been checked.
2. Click the Enable WEP Wireless Security checkbox.
3. From the drop-down menu, select an Authentication Type: *Open*, *Shared*, or *Both*.
4. Select a key by clicking a radio button on the left, select an encryption level from the drop-down menu on the right, and then enter the proper-length key. (Key length is outlined at the bottom of the window.)
5. Click **Apply**.

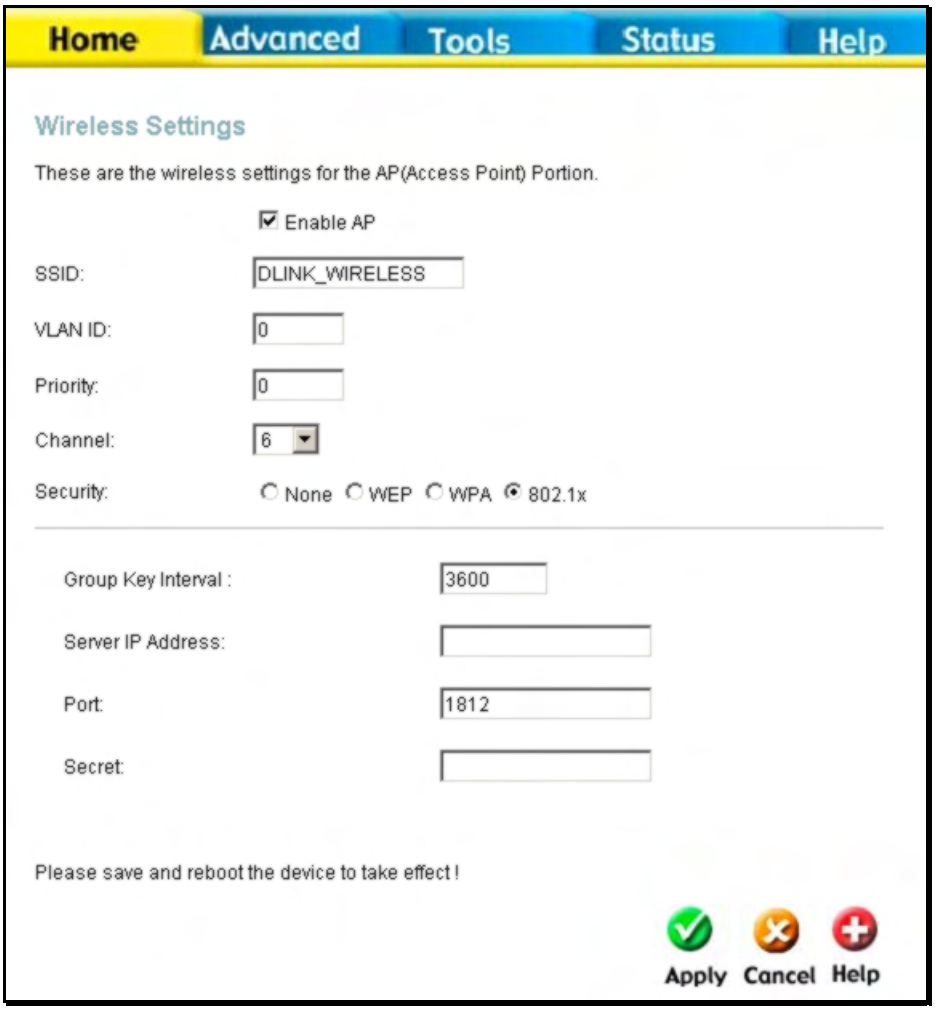
Notice *If encryption of any kind, at any level is applied to the Wireless network, all devices on the network must comply with all security measures.*

802.1x

Some network-security experts now recommend that wireless networks use 802.1X security measures to overcome some weaknesses in standard WEP applications. A RADIUS server is used to authenticate all potential users. Configure the following:

- **Server IP Address:** Enter the IP address of the Radius server.
- **Port:** Enter a port number, or accept the default.
- **Secret:** Enter a password (1-63 character).
- **Group Key Interval:** Time (in seconds) after which the Group Key is changed automatically (*1-99999*).

Notice *The values needed for 802.1x can be obtained from your Internet Service Provider (ISP).*

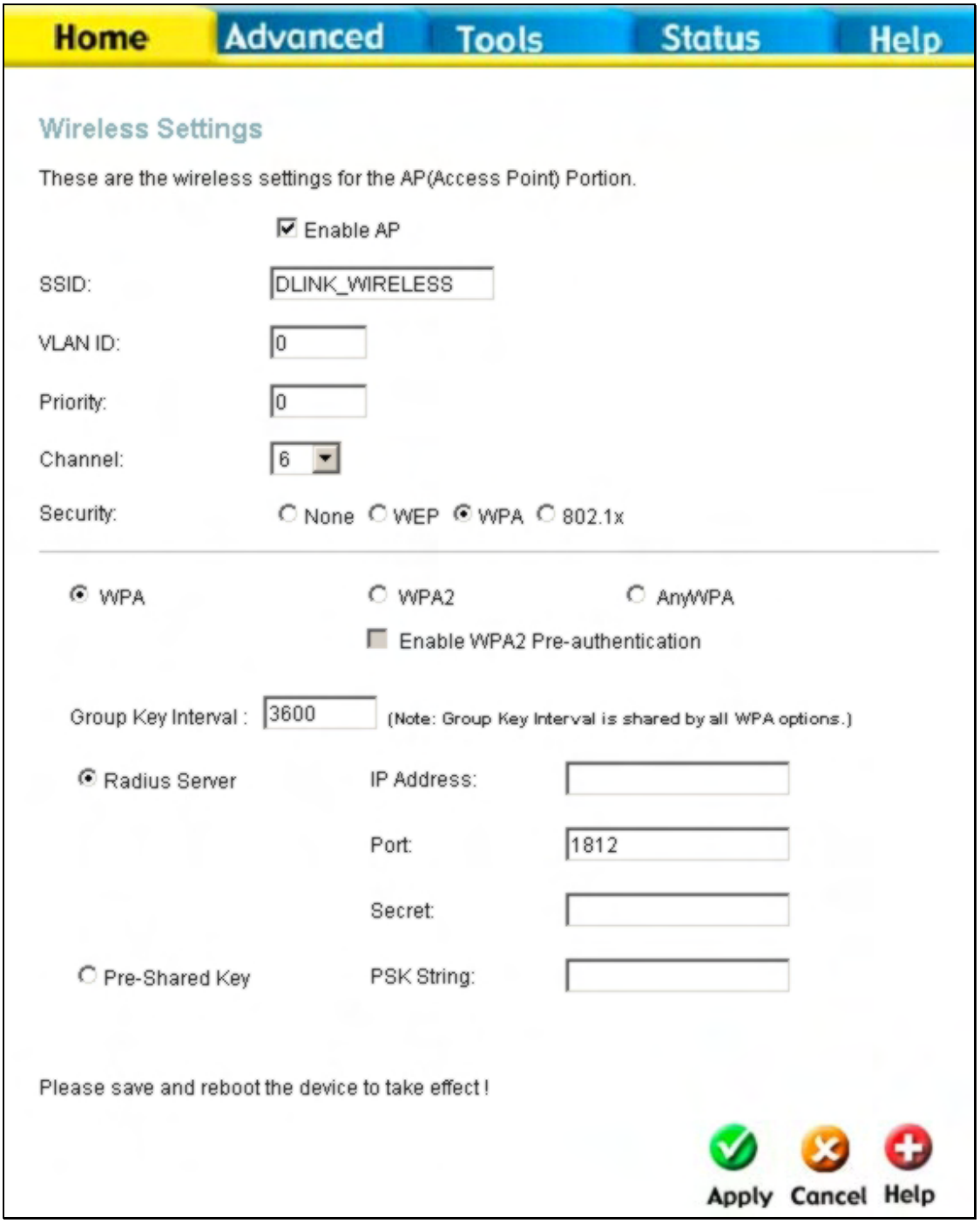


Wireless Settings menu– 802.1x

1. Make sure the **Enable AP** checkbox at the top of the window has been checked.
2. Click to select the **802.1x** radio button.
3. In the **Group Key Interval** entry field, enter a Time (in seconds) after which the Group Key is changed automatically.
4. Enter the **Server IP Address** of the RADIUS server.
5. Enter a Port number, or accept the default.
6. Enter a password or "Shared" **Secret** (1-63 characters).
7. Click **Apply**.

WPA (Wi-Fi Protected Access)

Wi-Fi Protected Access was designed to provide improved data encryption, perceived as weak in WEP, and to provide user authentication, largely nonexistent in WEP. There are two versions of WPA, both are supported by the Access Point. WPA includes the option of using a Pre-Shared Key similar to WEP, or a RADIUS server can be used for varification.



Wireless Settings menu – WPA

1. Make sure the **Enable AP** checkbox at the top of the window has been checked.

2. Click to select the **WPA** radio button.

3. In the **Group Key Interval** entry field, enter a Time (in seconds) after which the Group Key is changed automatically.

4. Select either **Radius Server** or **Pre-Shared Key** depending on the varification you are using for the Wireless network.

    a. If you are using a **Radius Server** for authentication, select the Radius Server button and enter the server **IP Address** of the RADIUS server, a **Port** number (or accept the default), and a "Shared" **Secret** (1-63 characters).

Notice *The values needed for Radiusauthentication can be obtained from your Internet Service Provider (ISP).*

    b. If you are using a **Pre-Shared Key**, type an alphanumeric value of 1-63 characters in length used for authentication.

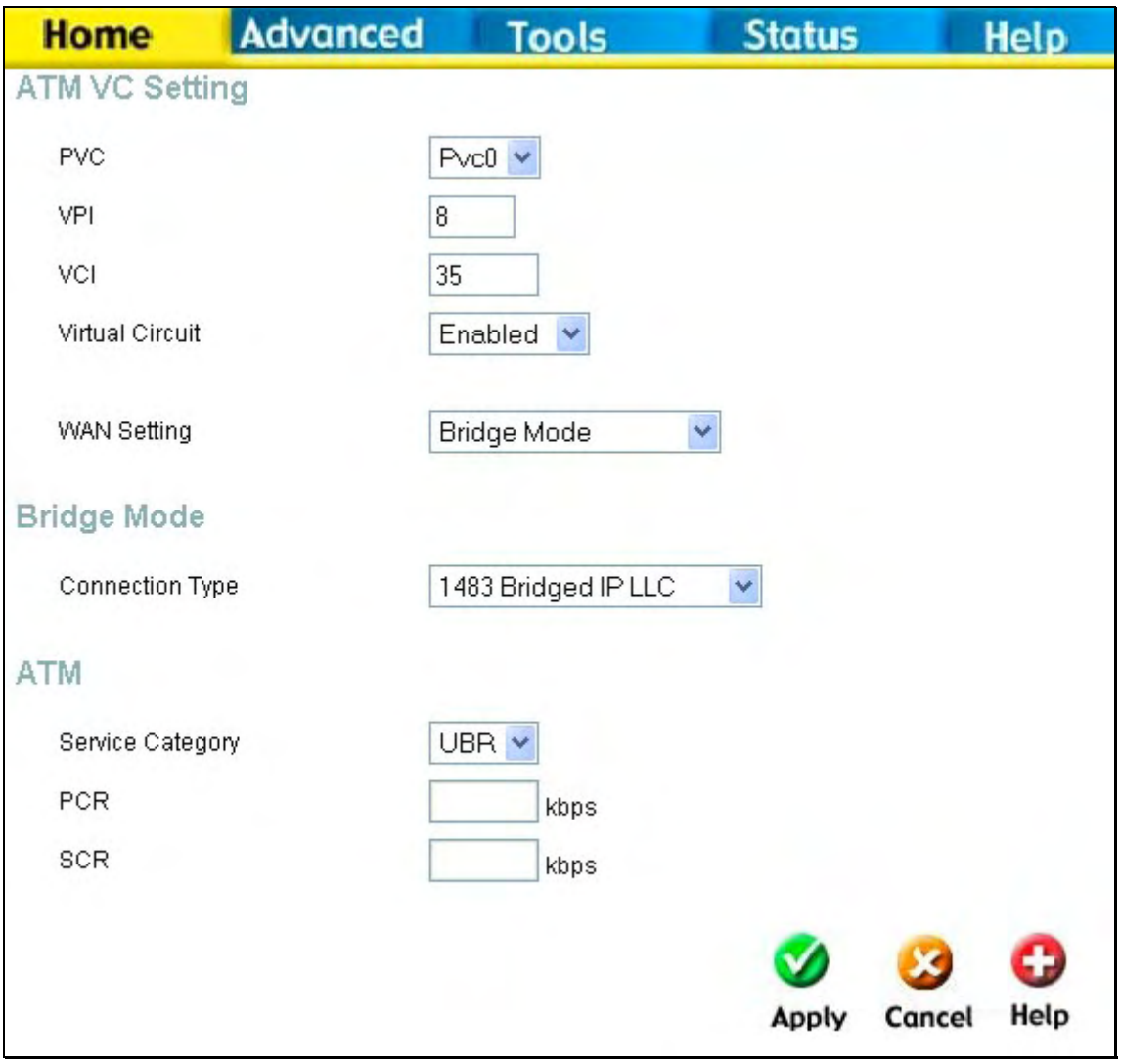
5. Click **Apply**.

WAN

To configure the Router's basic configuration settings without running the Setup Wizard, you can access the windows used to configure WAN, LAN, DHCP, and DNS settings directly from the **Home** directory. To access the WAN Settings window, click on the **WAN** link button on the left side of the first window that appears when you successfully access the web manager.

Bridge Mode

The WAN Settings window is also used to configure the Router for multiple virtual connections (Multiple PVCs).



WAN Settings window – Bridge Mode

Select the connection type used for your account. The window will display settings that are appropriate for the connection type you select. Follow the instruction below according to the type of connection you select in the WAN Settings window.

For Bridged connections it will be necessary for most users to install additional software on any computer that will the Router for Internet access. The additional software is used for the purpose of identifying and verifying your account, and then granting Internet access to the computer requesting the connection. The connection software requires the user to enter the User Name and Password for the ISP account. This information is stored on the computer, not in the Router.

Follow the instructions below to configure a Bridged connection for the WAN interface.

To configure a Dynamic IP Address connection, perform the steps listed below. Some of the settings do not need to be changed the first time the device is set up, but can be changed later if you choose. See the table below for a description of all the settings available in this window.

1. Choose the **Bridge Mode** option from the **WAN Settings** pull-down menu.

2. Under the **ATM VC Settings** at the top of the window should not be changed unless you have been instructed to change them. However, if you are instructed to change the **VPI** or **VCI** values, type in the values assigned for your account. Leave the **PVC** and **Virtual Circuit** setting at the default (*Pcv0* and *Enabled*) values for now. This can be used later if you are configuring multiple virtual circuits for your ADSL service. For more information on ATM VC Settings, see the table on page 45 below.

3. Under the **Bridge Mode** heading, choose the **Connection Type** from the pull-down menu. This defines both the connection type and encapsulation method used for your ADSL service. The available options are *1483 Bridged IP LLC* and *1483 Bridged IP VC-Mux.* If have not been provided specific information for the Connection Type setting, leave the default setting.

4. Most users will not need to change **ATM** settings. If this is the first time you are setting up the ADSL connection it is recommended that you leave the **Service Category** settings at the default values until you have established the connection. See the table on page 44 for a description of the parameters available for ATM traffic shaping.

5. When you are satisfied that all the WAN settings are configured correctly, click on the **Apply** button.

6. The new settings must be saved and the Router must be restarted for the settings to go into effect. To save and reboot the Router, click on the **Tools** directory tab and then click the **System** button. In the **System Settings** window, click the **Save and Reboot** button under Save Settings and Reboot the System.

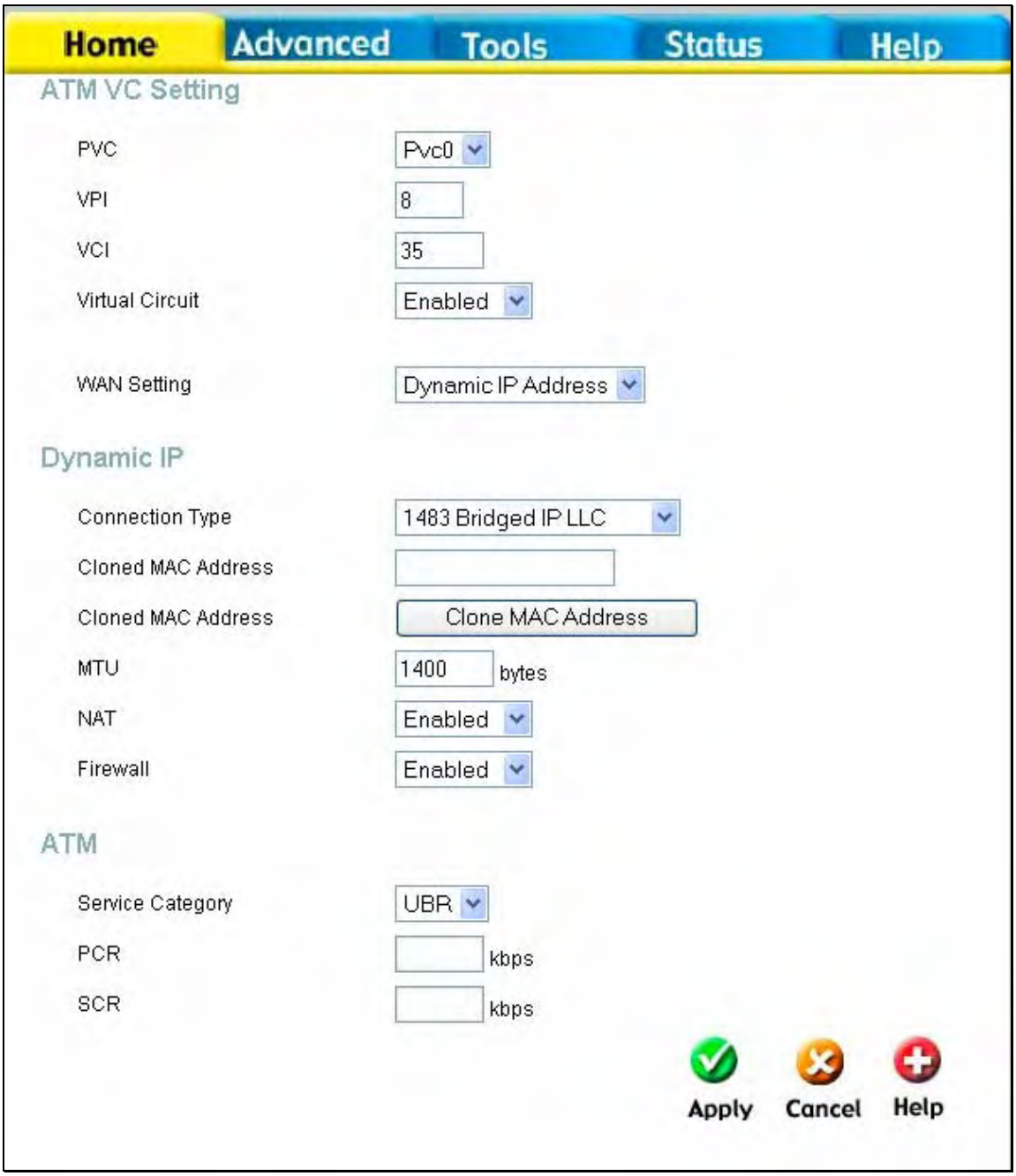
7. Click **OK** when the following “Save and restart?” dialog box opens.

8. The Router will save the new settings and restart. Upon restarting the Router will automatically establish the WAN connection.

Dynamic IP Address

A Dynamic IP Address connection configures the Router to automatically obtain its global IP address from a DHCP server on the ISP's network. The service provider assigns a global IP address from a pool of addresses available to the service provider. Typically the IP address assigned has a long lease time, so it will likely be the same address each time the Router requests an IP address.

To configure a Dynamic IP Address connection, perform the steps listed below. Some of the settings do not need to be changed the first time the device is set up, but can be changed later if you choose. See the table below for a description of all the settings available in this window.



WAN Settings window – Dynamic IP Address

To configure a Dynamic IP Address connection for the WAN, follow these steps:

1. Choose the **Dynamic IP Address** option from the **WAN Settings** pull-down menu.
2. Under the **ATM VC Settings** at the top of the window should not be changed unless you have been instructed to change them. However, if you are instructed to change the **VPI** or **VCI** values, type in the values assigned for your account. Leave the **PVC** and **Virtual Circuit** setting at the default (*Pcv0* and *Enabled*) values for now. This can be used later if you are configuring multiple virtual circuits for your ADSL service. For more information on ATM VC Settings, see the table on page 45 below.
3. Under the **Dynamic IP** heading, choose the **Connection Type** from the pull-down menu. This defines both the connection type and encapsulation method used for your ADSL service. The available options are *1483 Bridged IP LLC* and *1483 Bridged IP VC-Mux*. If have not been provided specific information for the Connection Type setting, leave the default setting.
4. Some ISPs record the unique MAC address of your computer's Ethernet adapter when you first access their network. This can prevent the Router (which has a different MAC address) from being allowed access to the ISPs network (and the Internet). To clone the MAC address of your computer's Ethernet adapter, type in the MAC address in the **Cloned MAC Address** field and click the **Clone MAC Address** button.
5. Leave the **MTU** value at the default setting (default = *1400*) unless you have specific reasons to change this (see table below).
6. **NAT** should remain *Enabled*. If you disable NAT, you will not be able to use more than one computer for Internet connections. NAT is enabled and disabled system-wide, therefore if you are using multiple virtual connections, NAT will disabled on all connections.
7. The **Firewall** should remain enabled for most users. If you choose to disable this you will not be able to use the features configured in the **Firewall Configuration** and **Filters** windows located in the **Advanced** directory. See the next chapter for more details on these windows.
8. Most users will not need to change **ATM** settings. If this is the first time you are setting up the ADSL connection it is recommended that you leave the **Service Category** settings at the default values until you have established the connection. See the table on page 44 for a description of the parameters available for ATM traffic shaping.
9. When you are satisfied that all the WAN settings are configured correctly, click on the **Apply** button.
10. The new settings must be saved and the Router must be restarted for the settings to go into effect. To save and reboot the Router, click on the **Tools** directory tab and then click the **System** button. In the **System Settings** window, click the **Save and Reboot** button under Save Settings and Reboot the System.
11. Click **OK** when the following "Save and restart?" dialog box opens.

12. The Router will save the new settings and restart. Upon restarting the Router will automatically establish the WAN connection.

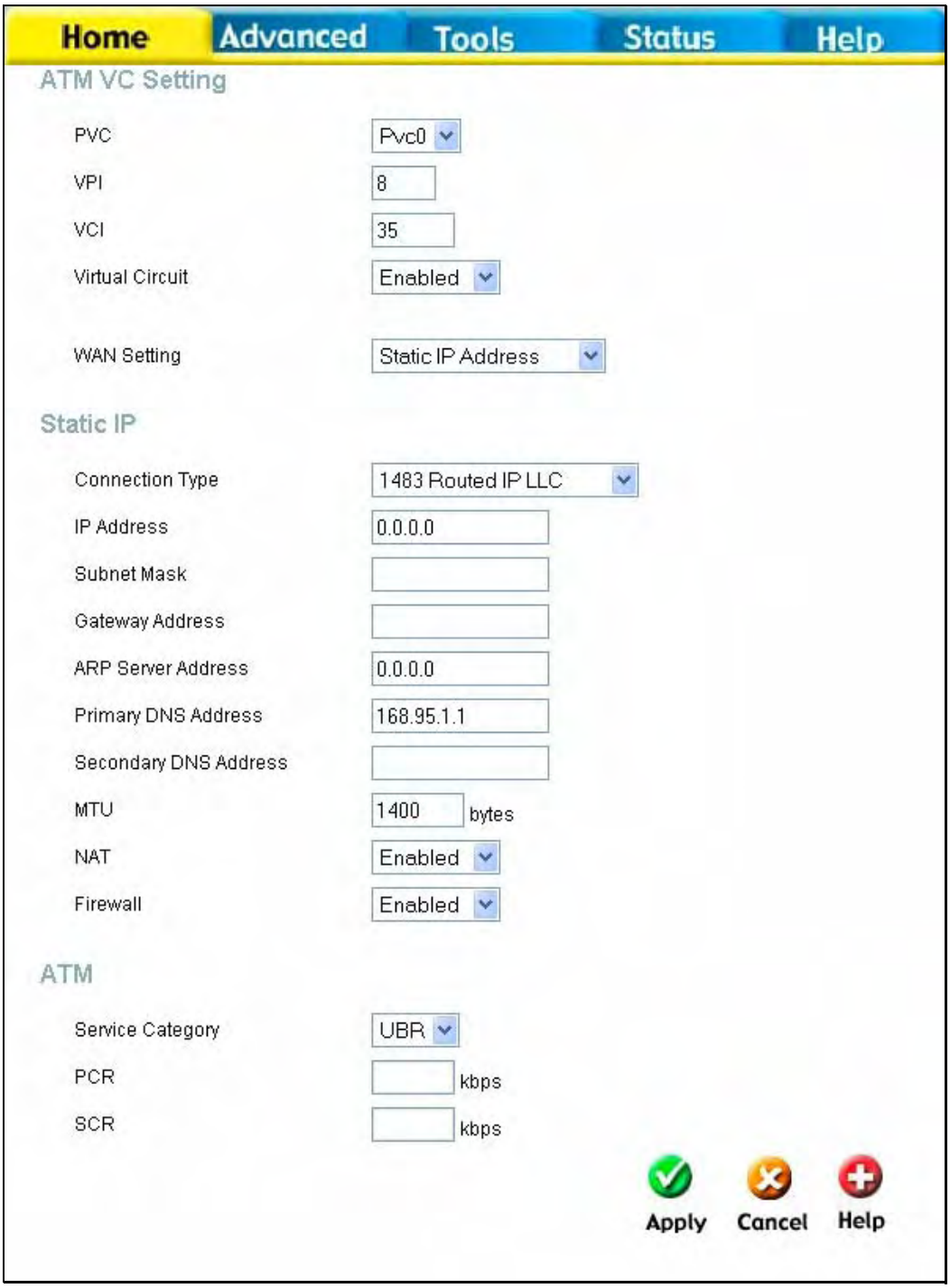
Additional settings for Dynamic IP Address connections:

Dynamic IP Parameters	Description
Connection Type	This specifies the connection type and encapsulation method used for your Dynamic IP Address connection. The options available are *Bridged IP LLC* or *Bridged IP VC-Mux*.
Cloned MAC Address	This is not always necessary, but may be required for some ISPs. Type in the MAC address of your computer's Ethernet adapter in the Cloned MAC Address field and click the **Clone MAC Address** button. This will copy the information to a file used by the Router to present to the ISP's server used for DHCP. Some ISPs record the unique MAC address of your computer's Ethernet adapter when you first access their network. If you want to later replace the cloned MAC address with the factory default setting, type in all zeros - 0:0:0:0:0:0 - and click the **Clone MAC Address** button.
Cloned MAC Address	To clone the MAC address of your computer's Ethernet adapter, type in the MAC address in the Cloned MAC Address field and then click this **Clone MAC Address** button.
MTU	The Maximum Transmission Unit size may be changed if you want to optimize efficiency for uploading data through the WAN interface. The default setting (1400 bytes) should be suitable for most users. Some user may want to adjust the setting to optimize performance for wireless traffic or when low latency is desired (such as with Internet gaming). It is highly recommended that the user research how adjusting the MTU may affect network traffic for better or worse.
NAT	Network Address Translation may be enabled or disabled with the pull-down menu. Keep in mind that disabling NAT allows only a single computer to be used for Internet access through the Router. NAT is enabled and disabled for the Router on all connections (i.e. Pvc0 – Pvc7) if your Router is set up for multiple virtual connections.
Firewall	Use this to universally enable or disable the Firewall and Filter features available in the Router. If you disable this you will not be able to configure settings in the **Firewall Configuration** window or **Filters** windows in the **Advanced** directory.

Static IP Address

When the Router is configured to use Static IP Address assignment for the WAN connection, you must manually assign a global IP Address, Subnet Mask and Gateway IP Address used for the WAN connection. Most users will also need to configure DNS server IP settings in the **DNS Configuration** window (see below). Follow the instruction below to configure the Router to use Static IP Address assignment for the WAN connection.

To configure a Static IP Address connection, perform the steps listed below. Some of the settings do not need to be changed the first time the device is set up, but can be changed later if you choose. See the table below for a description of all the settings available in this window.



WAN Settings window - Static IP

To configure a Static IP type connection for the WAN, follow these steps:

1. Choose the **Static IP Address** option from the **WAN Settings** pull-down menu.

2. Under the **ATM VC Settings** at the top of the window should not be changed unless you have been instructed to change them. However, if you are instructed to change the **VPI** or **VCI** values, type in the values assigned for your account. Leave the **PVC** and **Virtual Circuit** setting at the default (*Pcv0* and *Enabled*) values for now. This can be used later if you are configuring multiple virtual circuits for your ADSL service. For more information on ATM VC Settings, see the table on page 45 below.

3. Under the **Static IP** heading, choose the **Connection Type** from the pull-down menu. This defines both the connection type and encapsulation method used for your ADSL service. The available options are *Bridged IP LLC*, *Bridged IP VC-Mux*, *Routed IP LLC*, *Routed IP VC-Mux* or *IPoA*. If have not been provided specific information for the Connection Type setting, leave the default setting.

4. Change the **IP Address**, **Subnet Mask**, **Gateway Address** and (if available) **Secondary DNS** Server IP address as instructed by your ISP. These are the global IP settings for the WAN interface. This is the "visible" IP address of your account. Your ISP should have provided these IP settings to you. For IPoA (Classic IP over ATM) connections you may need to type in an additional IP address for a **ARP Server Address**. If you are using an IPoA connection, ask your ISP if it is necessary to use an ARP (Address Resolution Protocol) server.

5. Leave the **MTU** value at the default setting (default = *1400*) unless you have specific reasons to change this (see table below).

6. **NAT** should remain *Enabled*. If you disable NAT, you will not be able to use more than one computer for Internet connections. NAT is enabled and disabled system-wide, therefore if you are using multiple virtual connections, NAT will be disabled on all connections.

7. The **Firewall** should remain enabled for most users. If you choose to disable this you will not be able to use the features configured in the **Firewall Configuration** and **Filters** window located in the **Advanced** directory. See the next chapter for more details on these windows.

8. Most users will not need to change **ATM** settings. If this is the first time you are setting up the ADSL connection it is recommended that you leave the **Service Category** settings at the default values until you have established the connection. See the table on page 44 for a description of the parameters available for ATM traffic shaping.

9. When you are satisfied that all the WAN settings are configured correctly, click on the **Apply** button.

10. The new settings must be saved and the Router must be restarted for the settings to go into effect. To save and reboot the Router, click on the **Tools** directory tab and then click the **System** button. In the **System Settings** window, click the **Save and Reboot** button under Save Settings and Reboot the System.

11. Click **OK** when the following "Save and restart?" dialog box opens.

12. The Router will save the new settings and restart. Upon restarting the Router will automatically establish the WAN connection.

Additional settings for Static IP Address connections:

Static IP Parameters	Description
Connection Type	This specifies the connection type and the encapsulation method used for your Static IP Address connection. The options available are *Bridged IP LLC*, *Bridged IP VC-Mux*, *Routed IP LLC*, *Routed IP VC-Mux* or *IPoA*.
IP Address	This is the permanent global IP address for your account. This is the address that is visible outside your private network. Get this from your ISP.
Subnet Mask	This is the Subnet mask for the WAN interface. Get this from your ISP.
Gateway Address	This is the IP address of your ISP's Gateway router. It provides the connection to the Router for IP routed traffic that is outside your ISP's network. That is, this will be the primary connection from the Router to most of the Internet. Get this IP address from your ISP.
ARP Server Address (IPoA connection only)	This is not required for all IPoA connections. Check with your ISP for an ARP server IP address if this is necessary for your IPoA connection.
Primary DNS Address	This is the IP address of the first choice for Domain Name Service (DNS) used to match the named URL web address used by most browsers with the actual global IP address used for a web server. Usually this will be a server owned by the ISP. Get this IP address from your ISP.
Secondary DNS Address	This is the second choice for a DNS server. Get this IP address from your ISP.
MTU	The Maximum Transmission Unit size may be changed if you want to optimize efficiency for uploading data through the WAN interface. The default setting (*1400* bytes) should be suitable for most users. Some user may want to adjust the setting to optimize performance for wireless traffic or when low latency is desired (such as with Internet gaming). It is highly recommended that the user research how adjusting the MTU may affect network traffic for better or worse.
NAT	Network Address Translation may be enabled or disabled with the pull-down menu. Keep in mind that disabling NAT allows on a single computer to be used for Internet access through the Router. NAT is enabled and disabled for the Router on all connections (i.e. Pvc0 – Pvc7) if your Router is set up for multiple virtual connections.
Firewall	Use this to universally enable or disable the Firewall and Filter features available in the Router. If you disable this you will not be able to configure settings in the **Firewall Configuration** window or the **Filters** window in the **Advanced** directory.

PPPoE/PPPoA

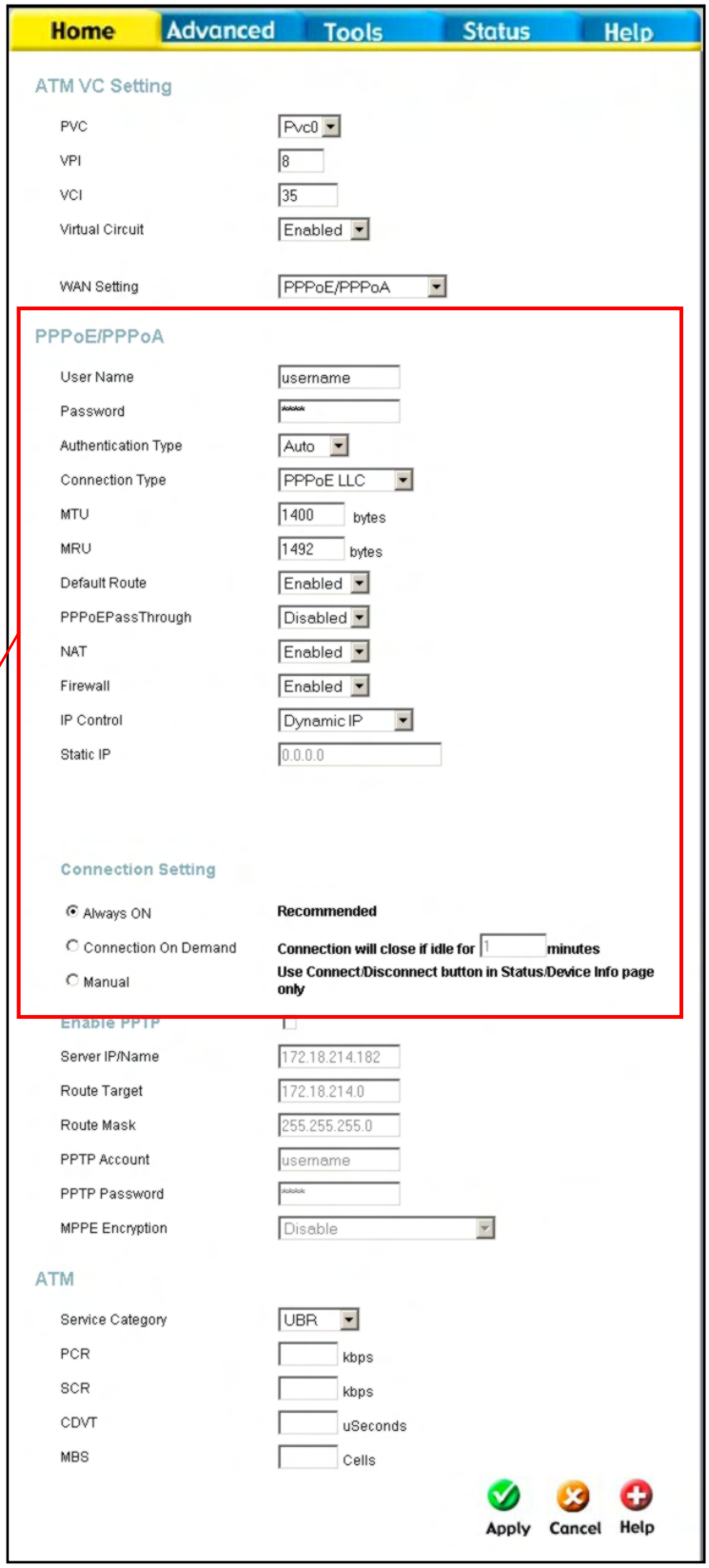
Follow the instructions below to configure the Router to use a PPPoE or PPPoA for the Internet connection. Make sure you have all the necessary information before you configure the WAN connection.

Most user will only need to change some or all of the settings listed under **PPPoE/PPPoA** and **Connection Setting** heading in the WAN settings menu. This area is contained within the red square in the example to the right. An enlarged view of this section can be seen on the next page followed by step-by-step instructions on how to configure WAN settings for a PPPoE or PPPoA connection.

Note

Most users with PPPoE/PPPoA connections only need to configure the settings caontained within the red square in this example menu.

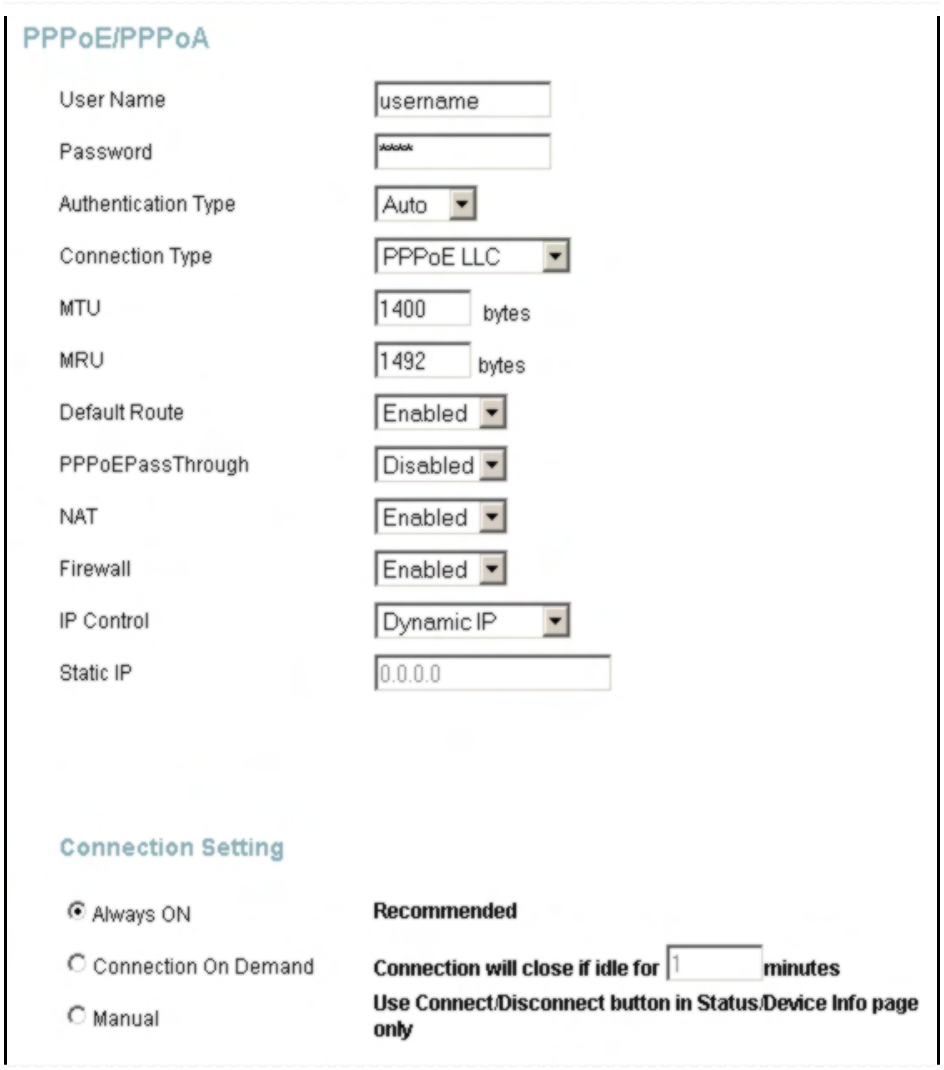
See enlarged view of this section below.



WAN Settings menu – PPPoE/PPPoA (entire menu)

PPPoE and PPPoA Settings in detail

The example menu below is a section of the WAN settings for PPPoE and PPPoA connection types. Most users will only need to enter a **User Name** and **Password**.



PPPoE/PPPoA WAN settings section (enlarged view)

To configure a PPPoE or PPPoA type WAN connection, follow these steps:

1. If not already selected, choose the *PPPoE/PPPoA* option from the **WAN Settings** pull-down menu. PPPoE/PPPoA is selected by default if you are configuring the Router for the first time.

2. Under the **ATM VC Settings** at the top of the window should not be changed unless you have been instructed to change them. However, if you are instructed to change the **VPI** or **VCI** values, type in the values assigned for your account. Leave the **PVC** and **Virtual Circuit** setting at the default (*Pcv0* and *Enabled*) values for now. This can be used later if you are configuring multiple virtual circuits for your ADSL service. For more information on ATM VC Settings, see the table on page 45 below.

3. Under the **PPPoE/PPPoA** heading, type the **User Name** and **Password** used for your ADSL account. A typical User Name will be in the form user1234@isp.co.uk. The Password may be assigned to you by your ISP or you may have selected it when you set up the account with your ISP.

4. Choose the correct **Authentication Type** from the drop-down menu. Most users will want to leave the setting on *Auto*. *PAP* and *CHAP* are the other two options. The *Auto* setting will automatically detect the correct type of authentication.

5. Choose the **Connection Type** from the pull-down menu located under the User Name and Password entry fields. This defines both the connection protocol and encapsulation method used for your ADSL service. The available options are *PPPoA VC-Mux*, *PPPoA LLC* and *PPPoE LLC*. If have not been provided specific information for the Connection Type setting, leave the default setting.

6. Leave the **MTU** value at the default setting (default = *1400*) unless you have specific reasons to change this (see table below for more information).

7. Leave the **MRU** value at the default setting (default = *1492*) unless you have specific reasons to change this (see table below for more information).

8. Leave the **Default Route** enabled if you want to use the Router as the default route to the Internet for your LAN. Whenever a computer on the LAN attempts to access the Internet, the Router becomes the Internet gateway to the computer. If you have an alternative route for Internet traffic you may disable this without effecting the Router's connection.

9. Enable **PPPoE PassThrough** if you want the Router to allow a "dial-up" or separate bridged PPP connection to an individual PC (see table below for more information).

10. **NAT** should remain *Enabled*. If you disable NAT, you will not be able to use more than one computer for Internet connections. If you are using multiple virtual connections, NAT functions system-wide, therefore if t is disabled, NAT will disabled on all connections.

11. The **Firewall** should remain enabled for most users. If you choose to disable this you will not be able to use the features configured in the **Firewall Configuration** and **Filters** windows located in the **Advanced** directory. The next chapter contains a separate section describing these Advanced features.

12. Typically the globally IP settings (i.e. IP address for the WAN interface) for a PPPoA or PPPoA connection will use Dynamic IP assignment from the ISP. Some accounts may be assigned a specific global IP address. If you have been give an IP address for you PPPoE/PPPoA connection, select the **Static IP** option from the **IP Control** pull-down menu. This menu can be used to configure the WAN port as an Unnumbered IP interface. (See table below for information on Unnumbered IP).

13. Choose the desired **Connection Setting**. Select from: Always ON, Connection On Demand, or Manual. Most users will want to choose the default connection setting, Always ON.

14. Point-to-Point Tunneling Protocol is a pass-through mechanism that allows packets to pass through the Router so that it effectively functions as a bridge. Check **Enable PPTP** and enter the required information in the **ServerIP/Name**, **Route Target**, **Route Mask**, **PPTP Account**, **PPTP Password**, and **MPPE Encryption** fields.

15. Most users will not need to change **ATM** settings. If this is the first time you are setting up the ADSL connection it is recommended that you leave the **Service Category** settings at the default values until you have established the connection. See the table on page 44 for a description of the parameters available for ATM traffic shaping.

16. When you are satisfied that all the WAN settings are configured correctly, click on the **Apply** button.

17. The new settings must be saved and the Router must be restarted for the settings to go into effect. To save and reboot the Router, click on the **Tools** directory tab and then click the **System** button. In the **System Settings** window, click the **Save and Reboot** button under Save Settings and Reboot the System.

18. Click **OK** when the following "Save and restart?" dialog box opens.

19. The Router will save the new settings and restart. Upon restarting the Router will automatically establish the WAN connection.

PPPoE/PPPoA Parameters	Description
User Name	For PPP connections, a User Name and Password are used to identify and verify your account to the ISP. Enter the User Name for your ADSL service account. User names and passwords are case-sensitive, so enter this information exactly as given to you by your ISP.
Password	Together with the User Name, this is used to verify your account to the ISP. Enter the Password exactly as given to you by your ISP.
Connection Type	This specifies the protocol (PPPoE or PPPoA) and the encapsulation method (LLC or VC-Mux) used for your connection. The options available are *PPPoE LLC*, *PPPoA LLC* or *PPPoA VC-Mux*.
MTU	The Maximum Transmission Unit size may be changed if you want to optimize efficiency for uploading data through the WAN interface. The default setting (*1400* bytes) should be suitable for most users. Some user may want to adjust the setting to optimize performance for wireless traffic or when low latency is desired (such as with Internet gaming). It is highly recommended that the user research how adjusting the MTU may effect network traffic for better or worse.
MRU	Similar to the MTU, except this applies to Maximum Received Unit size for downloading data. Most users will be happy with the default setting (*1492* bytes). However this may also be optimized for fast downloads of general bulk Internet traffic, for low latency or for downloading to computers on the Wireless LAN. As with the MTU setting, the user should carefully consider how changing the MRU may affect Internet downloads for all systems on your LAN.
Default Route	When this is enabled, the Router will be considered to be the primary gateway to the Internet and WAN for systems on your network. If you are using the Router on a network with one or more alternative gateway routers, you may prefer to disable this if you will use another router as the primary gateway.
PPPoE PassThrough	This feature enables the Router to allow a "dial-up" or separate bridged PPP connection to an individual PC. In this instance the Router will serve as a bridge.
NAT	Network Address Translation may be enabled or disabled with the pull-down menu. Keep in mind that disabling NAT allows only a single computer to be used for Internet access through the Router. NAT is enabled and disabled for the Router on all connections (i.e. Pvc0 – Pvc7) if your Router is set up for multiple virtual connections.
Firewall	Use this to universally enable or disable the Firewall and Filter features available in the Router. If you disable this you will not be able to configure settings in the **Firewall Configuration** window or **Filters** window in the **Advanced** directory.
IP Control	This is used to determine how global IP settings are handled for the WAN interface. Typically PPPoE or PPPoA connections will use the default setting for *Dynamic IP*. Some users will be given a specific IP address for the WAN interface. In this case you need to change this setting to *Static IP*. When Static IP is selected in the IP Control menu, you need to type in the global IP address provided to you by your ISP. The *IP Unnumbered* option is used if you want to set up a non-TCP/IP port protocol link through the WAN interface. An IP Unnumbered interface does not have an IP address and therefore cannot be managed via Telnet or any other TCP/IP application.
Static IP	If you have selected the *Static IP* option in the IP Control menu, type in the global IP address used for your WAN interface. Your ISP should provide this IP address to you.
Connection Setting	Select the desired option: Always ON, Connection On Demand, or Manual. Most users will want to choose the default connection setting, Always ON.

ATM Settings - Traffic Shaping

The ATM settings in the WAN Settings windows for the different connection types can be used to adjust QoS parameters for ADSL clients. This may not be available to all ADSL accounts.

ATM Settings for WAN connection

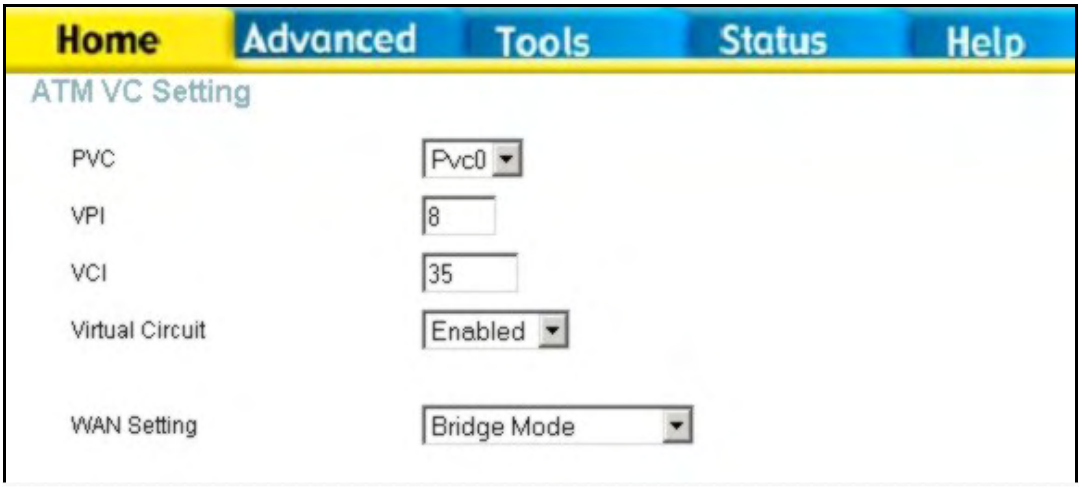
The table below provides a description of the ATM settings for traffic shaping.

ATM Parameters	Description
	The ATM settings allow the user to adjust ATM Quality of Service (QoS) or traffic parameters to suit specific traffic requirements. For applications or circumstances where packet loss or packet delay is a concern, ATM QoS can be adjusted to minimize problems. For most accounts, it will not be necessary to change these settings. Altering QoS settings can adversely affect performance of some commonly used Internet applications. If you plan to change QoS or traffic parameters, contact your ISP or network services provider for information on what types of adjustment are available or possible for your account. Your ISP may not support the class of service you want to use. To adjust ATM QoS parameters, select one of the Service Categories listed here and type in the PCR value in the entry field below. For the VBR service category, an additional parameter (SCR) must also be defined.
Service Category	*UBR* – Unspecified Bit Rate, this is the default category used for general-purpose Internet traffic where normal levels of packet loss and delay are acceptable. For some applications or for multiple connection accounts, it may be desirable to specify the PCR. *CBR* – Constant Bit Rate, usually used in circumstances where very low packet loss and very low Cell Delay Variable (CDV) are desirable. *VBR-nt* – Real-time Variable Bit Rate. This models bursty traffic with specified peak and sustainable rates. Please note that when VBR-rt is specified, both PCR and SCR are required (by ATM standards). *VBR-nrt* – Non-real-time Variable Bit Rate, usually used when network traffic is characterized by bursts of packets at variable intervals, and some moderate packet loss and delay is acceptable. This category is typically used for audio and video applications such as teleconferencing. The network must support QoS Class 2 to use VBR-nrt.

ATM Parameters (continued)	Description
PCR	Peak Cell Rate – The PCR is inversely related to the time interval between ATM cells. It is specified for all three service categories (UBR, CBR and VBR) in Kbps.
SCR	Sustainable Cell Rate – The SCR is defined for the VBR service category. This is the rate that can be sustained for "bursty", on-off traffic sources. It is a function of Maximum Burst Size (MBS) and the time interval (between cells).
CDVT	Cell Delay Variation Tolerance – CDVT is a measure of the cell clumping phenomenon by which cells are delayed in the network and are clumped together and arrive at a system at a faster rate than negotiated. Increasing the CDVT creates greater bucket depth.
MBS	Maximum Burst Size – The MBS is the maximum number of bytes that can be sent continuously from the source to the destination dropping any packets. Some ATM providers set the MBS and CDVT very low and adjust up if problems occur.

ATM VC Settings

ATM VC settings can be configured for all connection types in the WAN configuration menu of the Home directory.



ATM VC Settings in WAN Settings menu

The table below describes the ATM VC settings used to configure a PPPoE or PPPoA connection for an ADSL account.

ATM VC Parameters	Description
PVC	The Router supports using up to eight multiple virtual connections. This window allows the user to configure WAN settings for all the available connections (see instructions below on how to set up Multiple Virtual Connections). Use the PVC drop-down menu to select the connection (Pvc0 to Pvc7) you want to configure. Since most users will use only a single connection, the default setting *Pvc0* can be used for any changes made to the WAN settings.
VPI	The Virtual Path Identifier is used with the VCI to define a dedicated circuit on the ATM network portion of the connection to the Internet and WAN. Most users will not need to change this setting.
VCI	The Virtual Channel Identifier is used with the VPI to define a dedicated circuit on the ATM network portion of the connection to the Internet and WAN. Most users will not need to change this setting.
Virtual Circuit	As with the PVC setting, this is mainly for use by clients who are configuring the Router for multiple virtual connections. Use this to enable or disable the PVC you are currently configuring. By default, the Pvc0 is *Enabled* and the remaining PVCs are disabled.

LAN

You can configure the LAN IP address to suit your preference. Many users will find it convenient to use the default settings together with DHCP service to manage the IP settings for their private network. The IP address of the Router is the base address used for DHCP. In order to use the Router for DHCP on your LAN, the IP address pool used for DHCP must be compatible with the IP address of the Router. The IP addresses available in the DHCP IP address pool will change automatically if you change the IP address of the Router. See the next section for information on DHCP setup.

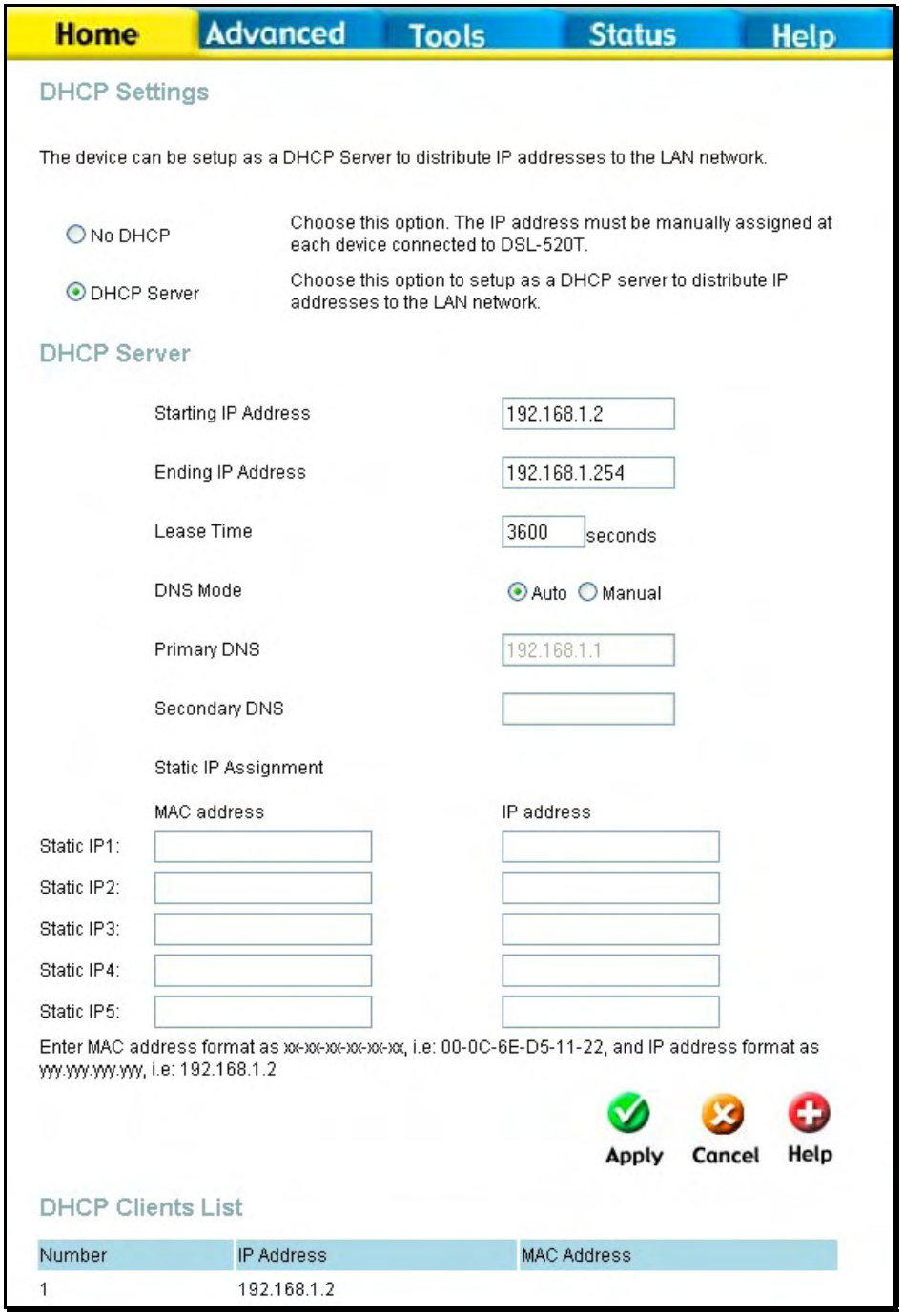
To access the **Management IP** window, click the **LAN** button in the **Home** directory.

Management IP window

To change the LAN **IP Address** or **Subnet Mask**, type in the desired values and click the **Apply** button. Your web browser should automatically be redirected to the new IP address. You will asked to login again to the Router's web manager.

DHCP

The DHCP server is enabled by default for the Router's Ethernet LAN interface. DHCP service will supply IP settings to workstations configured to automatically obtain IP settings that are connected to the Router though the Ethernet port. When the Router is used for DHCP it becomes the default gateway for DHCP client connected to it. Keep in mind that if you change the IP address of the Router the range of IP addresses in the pool used for DHCP on the LAN will also be changed. The IP address pool can be up to 253 IP addresses.



DHCP Settings window

To display the **DHCP Settings** window, click the **DHCP** button in the **Home** directory. Any active DHCP Clients appear at the bottom of the window in the DHCP Clients List. The IP address and MAC address for active DHCP clients are displayed in the list.

The two options for DHCP service are as follows:

- You may use the Router as a DHCP server for your LAN.
- You can disable DHCP service and manually configure IP settings for workstations.

You may also configure DNS settings for the LAN when using the Router in DHCP mode. In Auto **DNS Mode,** the Router will automatically relay DNS settings to properly configured DHCP clients. To manually enter DNS IP addresses, select the **Manual** DNS Mode option and type in a **Primary** and **Secondary DNS** IP Address in the field provided. The manually configured DNS settings will be supplied to clients that are configured to request them from the Router.

Follow the instructions below according to which of the above DHCP options you want to use. When you have configured the DHCP Settings as you want them, click the **Apply** button to commit the new settings.

Use the Router for DHCP

To use the built-in DHCP server, click to select the **DHCP Server** option if it is not already selected. The IP Address Pool settings can be adjusted. The **Starting IP Address** is the lowest available IP address (default = 192.168.1.2). If you change the IP address of the Router this will change automatically to be 1 more that the IP address of the Router.

The **Ending IP Address** is the highest IP address number in the pool. Type in the **Lease Time** in the entry field provided. This is the amount of time in seconds that a workstation is allowed to reserve an IP address in the pool if the workstation is disconnected from the network or powered off.

Disable the DHCP Server

To disable DHCP, click to select the **No DHCP** option and click on the **Apply** button. Choosing this option requires that workstations on the local network must be configured manually or use another DHCP server to obtain IP settings.

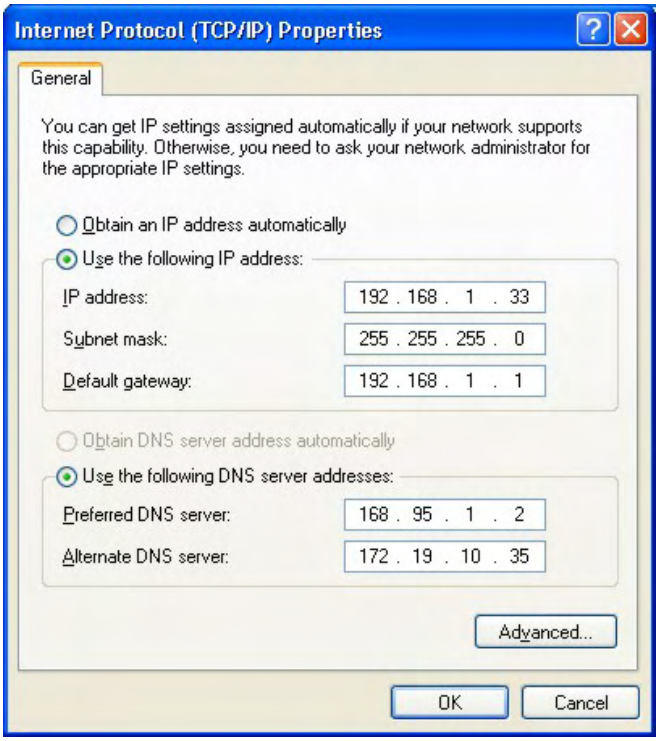
If you configure IP settings manually, make sure to use IP addresses in the subnet of the Router. You will need to use the Router's IP address as the Default Gateway for the workstation in order to provide Internet access.

Home
Advanced
Tools
Status
Help
DHCP Settings
The device can be setup as a DHCP Server to distribute IP addresses to the LAN network.
No DHCP
Choose this option. The IP address must be manually assigned at each device connected to DSL-522T.
DHCP Server
Choose this option to setup as a DHCP server to distribute IP addresses to the LAN network.
Apply
Cancel
Help

DHCP Settings window with DHCP disabled

Note

To manually configure IP settings on Windows workstations, open the TCP/IP Properties menu and select the "Use the following IP address" option. You will need to supply the IP addres, Subnet mask and Defualt gateway (use IP address of DSL-2640T) for each workstation. The example here also uses manually configured DNS settings.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 33
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 168 . 95 . 1 . 2
Alternate DNS server: 172 . 19 . 10 . 35
Advanced...
OK
Cancel

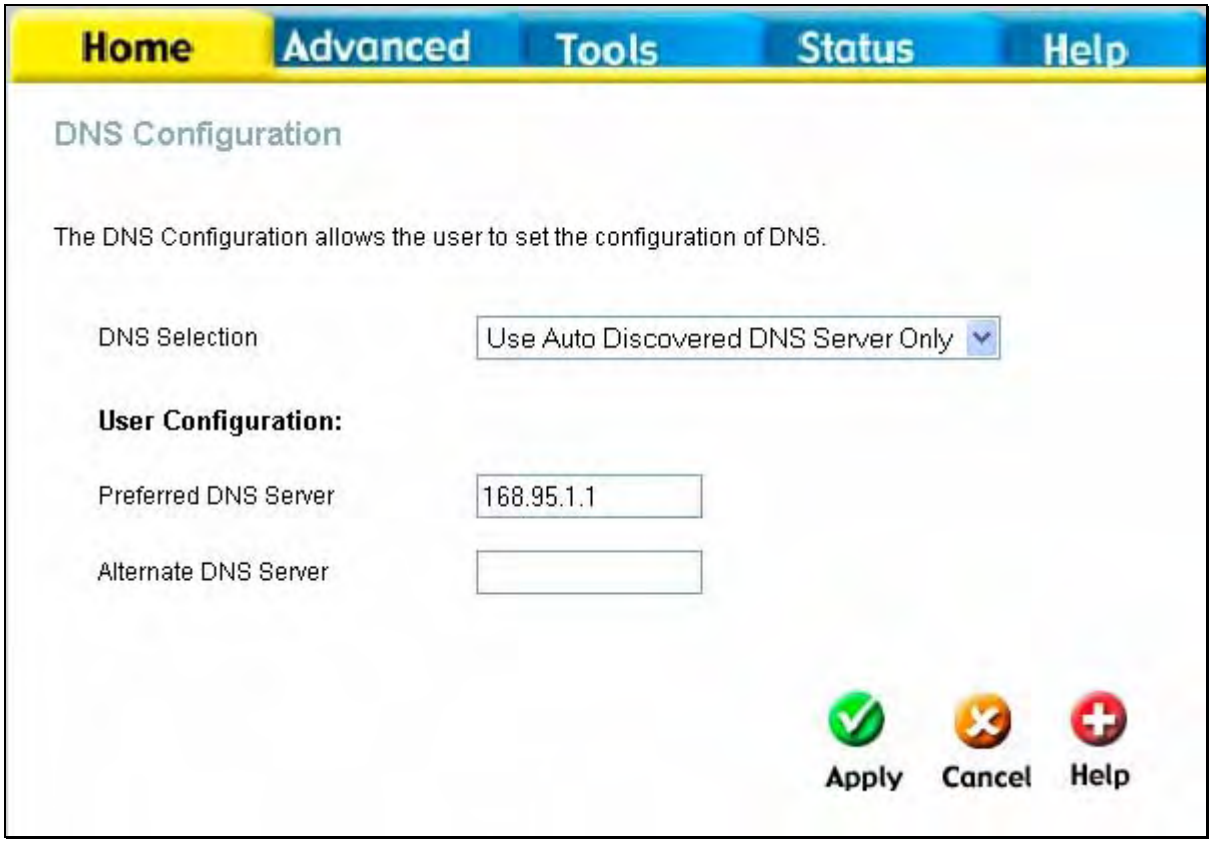
Static IP on LAN

If the Router has the DHCP server enabled it is possible to permanently assign IP addresses to workstations specified by their MAC address. Up to five IP addresses may be assigned to five different devices. This will take the chosen IP address used out of the available addresses in the dynamic IP address pool and give a permanent lease time for the IP address to the selected device.

To assign an IP address that will not age out, type in the **MAC Address** of the device and its static **IP Address** in the spaces provided. Use the format: 00-00-00-00-00-00 for the MAC address and the standard format: 192.168.0.xxx for the IP address. A Static DHCP Client List will appear below the DHCP Client list with any clients that have been configured for static IP address assignment.

DNS

The Router can be configured to relay DNS settings from your ISP or another available service to workstations on your LAN. When using DNS relay, the Router will accept DNS requests from hosts on the LAN and forward them to the ISP's, or alternative DNS servers. DNS relay can use auto discovery or the DNS IP address can be manually entered by the user. Alternatively, you may also disable the DNS relay and configure hosts on your LAN to use DNS servers directly. Most users who are using the Router for DHCP service on the LAN and are using DNS servers on the ISP's network, will leave DNS relay enabled (either auto discovery or user configured).



DNS Configuration window

In the DNS Relay Selection pull-down menu, choose to *Use Auto Discovered DNS Server Only*, *Use User Discovered DNS ServerOnly* or *Disable DNS Relay*.

If you have not been given specific DNS server IP addresses or if the Router is not pre-configured with DNS server information, select the *Use Auto Discovered DNS ServerOnly* option. Auto discovery DNS instructs the Router to automatically obtain the DNS IP address from the ISP through DHCP. If your WAN connection uses a Static IP address, auto discovery for DNS cannot be used.

If you have DNS IP addresses provided by your ISP, enter these IP addresses in the available entry fields for the **Preferred DNS Server** and the **Alternative DNS Server**.

If you choose to *Disable DNS Relay*, it will be necessary to configure DNS settings for hosts on the LAN since they will not be depending on the Router to forward the DNS requests.

When you have configured the DNS settings as desired, click the **Apply** button.

Note

*To use DNS Relay for computers on your local network, DNS Service Filtering must be disabled. See the **Firewall** section in the next chapter.*

Dynamic DNS

The Router supports DDNS (Dynamic Domain Name Service). The Dynamic DNS service allows a dynamic public IP address to be associated with a static host name in any of the many domains, allowing access to a specified host from various locations on the Internet. This is enabled to allow remote access to a host by clicking a hyperlinked URL in the form hostname.dyndns.org, Many ISPs assign public IP addresses using DHCP, this can make it difficult to locate a specific host on the LAN using standard DNS. If for example you are running a public web server or VPN server on your LAN, this ensures that the host can be located from the Internet if the public IP address changes. DDNS requires that an account be setup with one of the supported DDNS providers.

Dynamic DNS Configuration window

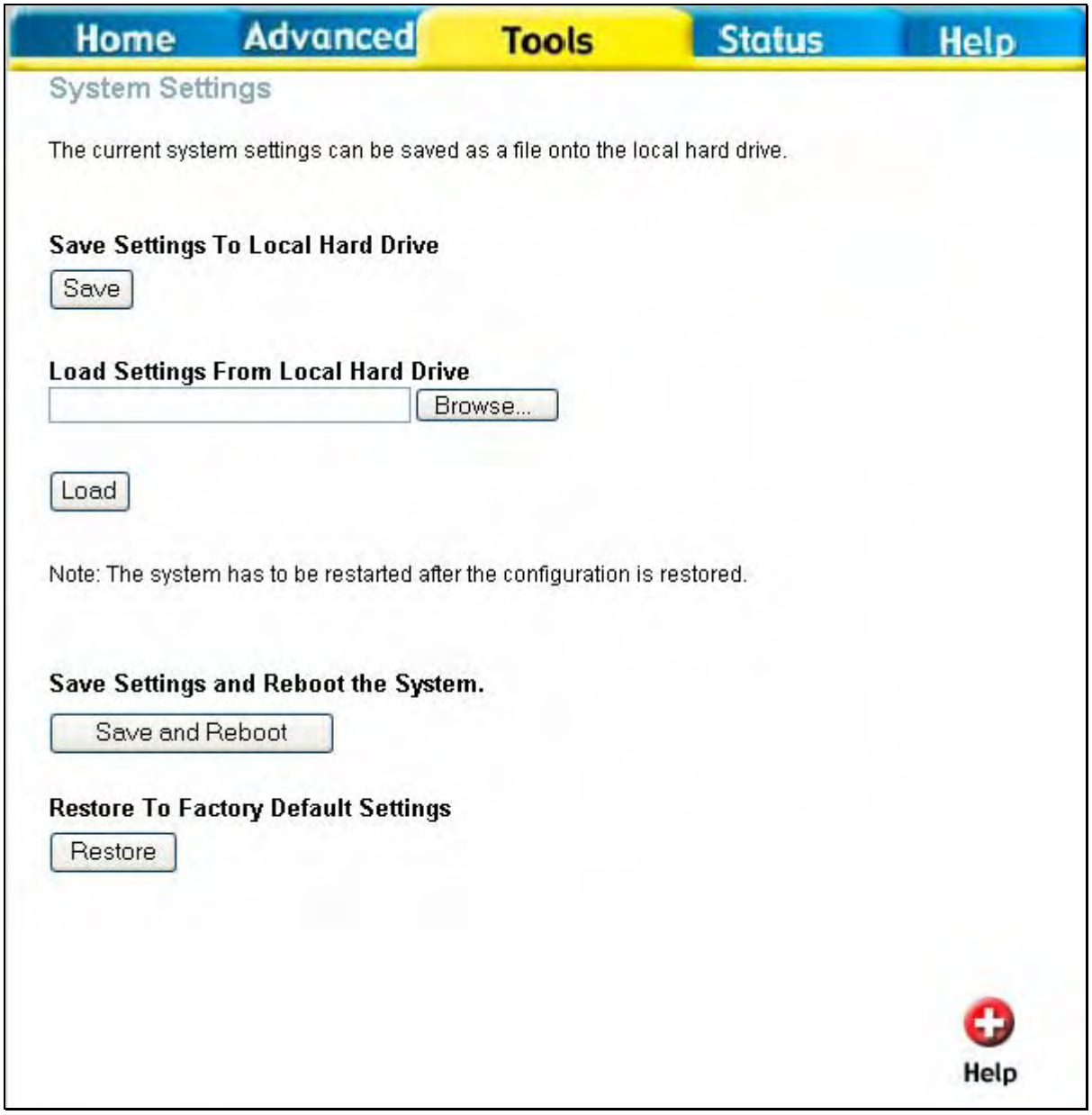
Note: DDNS requires that an account be setup with one of the supported DDNS servers prior to engaging it on the router. This function will not work without an accepted account with a DDNS server.

Enter the required DDNS information and click **Apply** to set this information in the Router.

DDNS Parameters	Description
DDNS Server	Select one of the DDNS registration organizations form those listed in the pull-down menu. Available servers include DynDns.org and No-IP.com.
Username (or Key)	Enter the username given to you by your DDNS server.
Password (or Key)	Enter the password or key given to you by your DDNS server
Host Name	Enter the host name of the DDNS server.

Save Settings and Reboot

When you have configured the DSL-2640T with the settings you desire, make sure you save those settings. To save the system configuration settings, click the **Tools** tab. You will be presented first with the **Administrator Settings** window. This window is described in the next chapter. To save the current configuration, click the **System** button to view the **System Settings** window pictured here.



System Settings window

To save the settings you have configured, click the **Save and Reboot** button under Save Settings and Reboot the System.

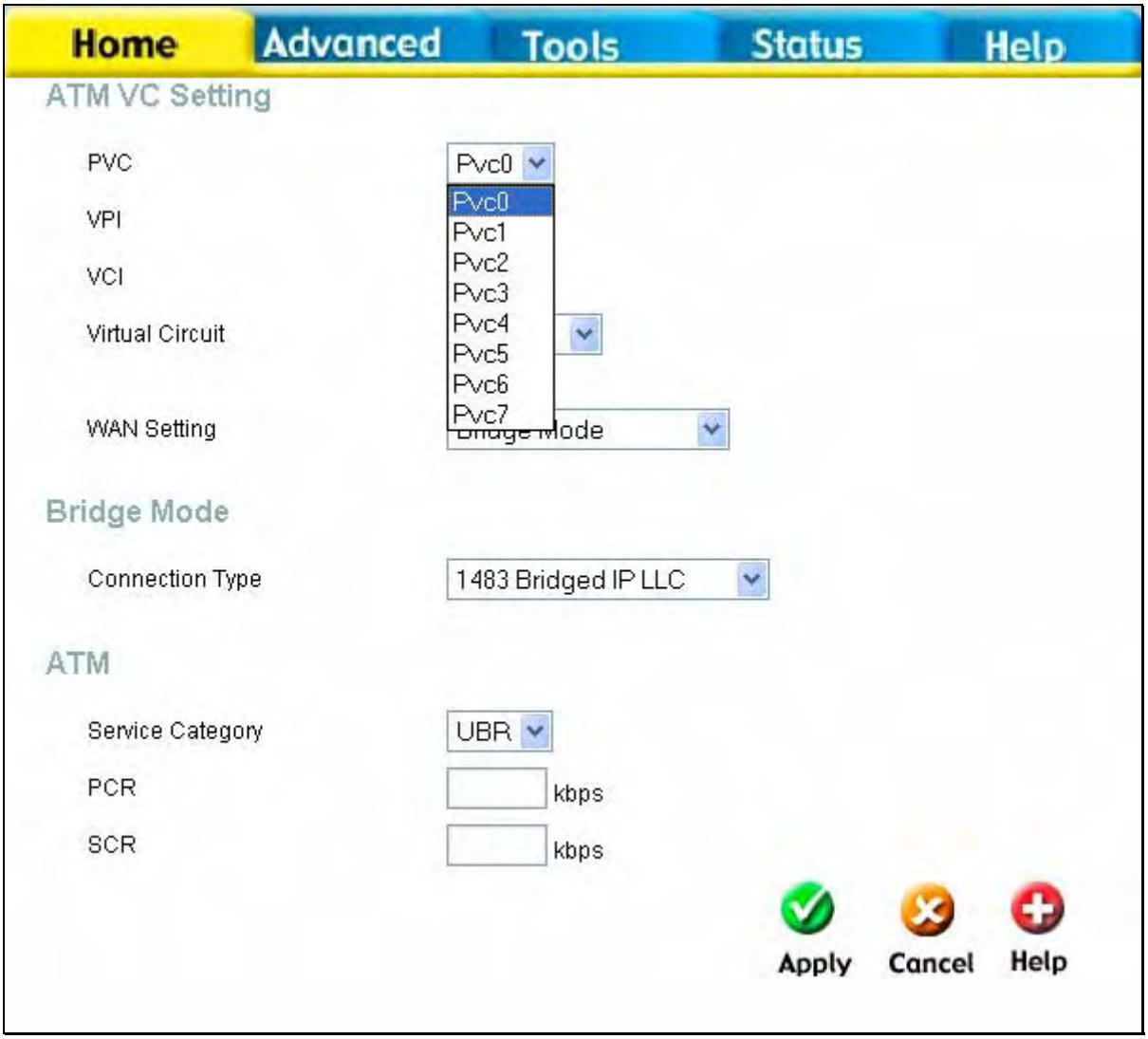
Multiple Virtual Connections

The Router supports multiple virtual connections. Up to eight PVCs to eight separate destinations can be created and operated simultaneously utilizing the same bandwidth. Additional PVC connections can be added for various purposes. For example, you may want to establish a private connection to remote office in order to create an extended LAN, or setup a server on a separate connection. Provisioning for additional PVC profiles must be done through your telecommunications services provider. Extended LAN operations employing multiple virtual connections require ADSL2+ routers or modems at the remote site for a successful connection. Contact your ISP or telecommunications service provider if you are interested in setting up multiple virtual connections.

After the necessary arrangements have been made to use the Router with multiple virtual connections, follow the instructions below to setup the Router using the VPI/VCI settings given to you by your server provider.

Configure Multiple PVCs

Additional PVCs can be configured by first accessing the WAN configuration window in the **Home** directory.



Select new PVC to configure in the WAN Settings window

The PVC pull-down menu offers eight virtual connections available for configuration. The default PVC used by the Router is labeled Pvc0. Any additional connections that are configured must have a VPI/VCI combination that is unique to the Router. These numbers will have been already been established by your service provider on their network.

To add a new virtual connection:

1. Select the new **PVC** to configure from the pull-down menu.
2. Enter the values for the **VPI** and **VCI** given to you by your service provider.
3. To activate the VC, select *Enabled* from the **Virtual Circuit** pull-down menu.
4. Configure the **WAN Settings** and **Connection Type** as desired.
5. To save the new settings, click the **Save and Reboot** button (**Tools > System**). The new connection will activate upon restarting.

In the example below, a new PVC (Pvc1) has been added using the WAN Settings window. The connection is setup as a bridged connection.

Configure new PVC

The new PVC that appears can be configured separately in other windows availailable in the **Advanced** directory.

4

Advanced Management

This chapter introduces and describes the management features that have not been presented in the previous chapter. These include the more advanced features used for network management and security as well as administrative tools to manage the Router, view statistics and other information used to examine performance and for troubleshooting.

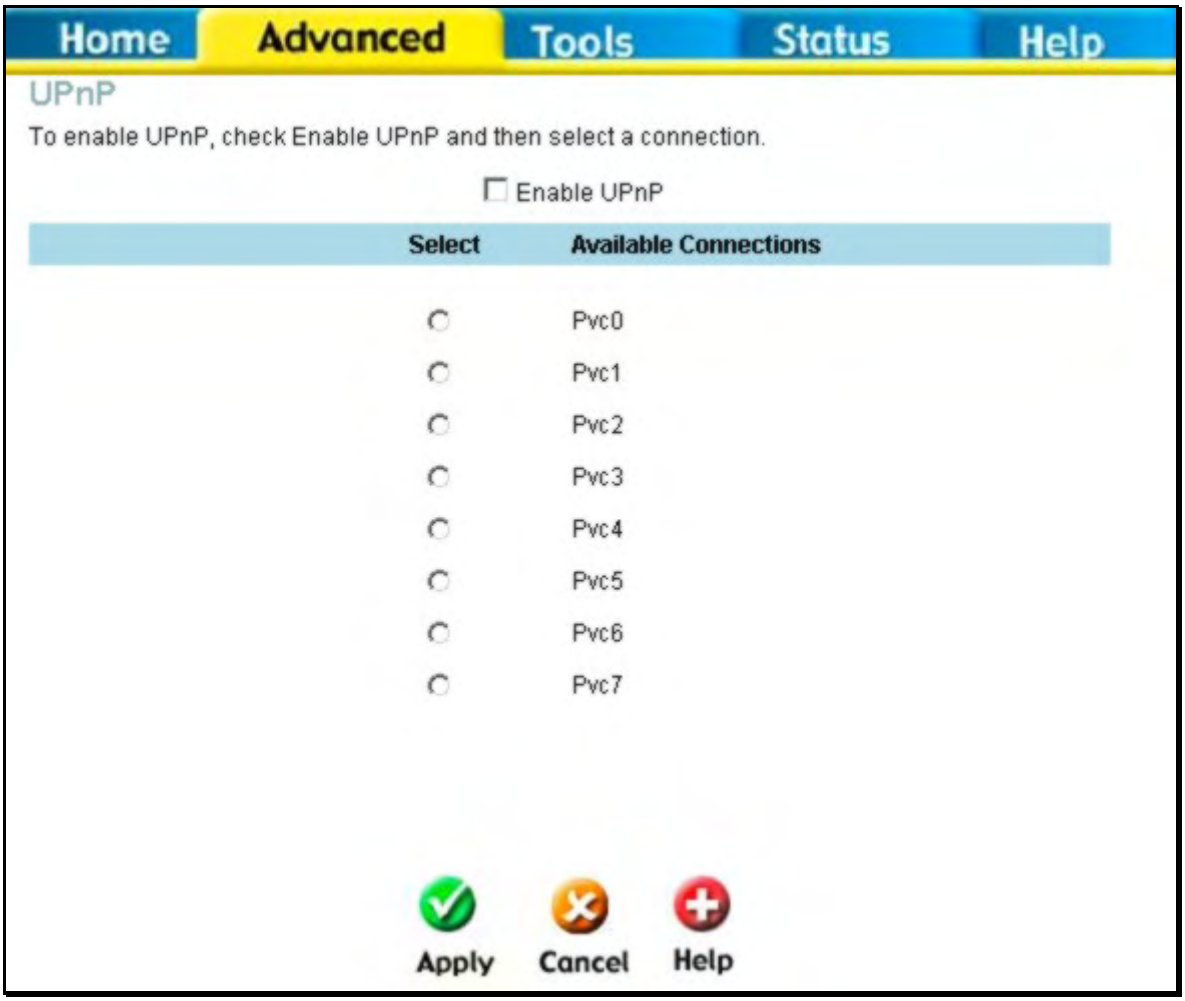
Use your mouse to click the directory tabs and window buttons in order to display the various configuration and read-only windows discussed below. The table below summarizes again the directories and menus available in the management web interface. In this chapter you will find descriptions for the windows located in the Advanced, Tools and Status directories.

Directory	Configuration and Read-only Windows
Home	Click the Home tab to access the Setup Wizard, WAN Settings, LAN Management IP Configuration, DHCP Settings for LAN Setup, DNS Configuration, and Dynamic DNS Configuration windows. See the previous chapter for a description of the Home directory windows.
Advanced	Click the Advanced tab to access the UPnP, Virtual Server, LAN Clients, SNMP Management, Filters, Bridge Filters, (Static) Routing Table, DMZ, Firewall Configuration, RIP Systemwide Configuration, PPP Connection, ADSL Configuration, and ATM VC Setting windows.
Tools	Click the Tools tab to access the Administrator Settings (used to set the system user name and password, backup and load settings), Time, Remote Log Settings, System Settings, Firmware Upgrade, Miscellaneous Configuration, and Diagnostic Test windows.
Status	Click the Status tab to view the Device Information, DHCP Clients, View Log, Traffic Statistics, and ADSL Status windows.
Help	The Help window presents links to pages that explain various functions and services provided by the Router.

UPnP

UPnP supports zero-configuration networking and automatic discovery for many types of networked devices. When enabled, it allows other devices that support UPnP to dynamically join a network, obtain an IP address, convey its capabilities, and learn about the presence and capabilities of other devices. DHCP and DNS service can also be used if available on the network. UPnP also allows supported devices to leave a network automatically without adverse effects to the device or other devices on the network.

UPnP is a protocol supported by diverse networking media including Ethernet, Firewire, phone line, and power line networking.



UPnP window

To enable UPnP for any available connection, click to check the **Enable UPnP** selection box, select the connection or connections on which you will enable UPnP listed under Available Connections and click the **Apply** button.

Virtual Server

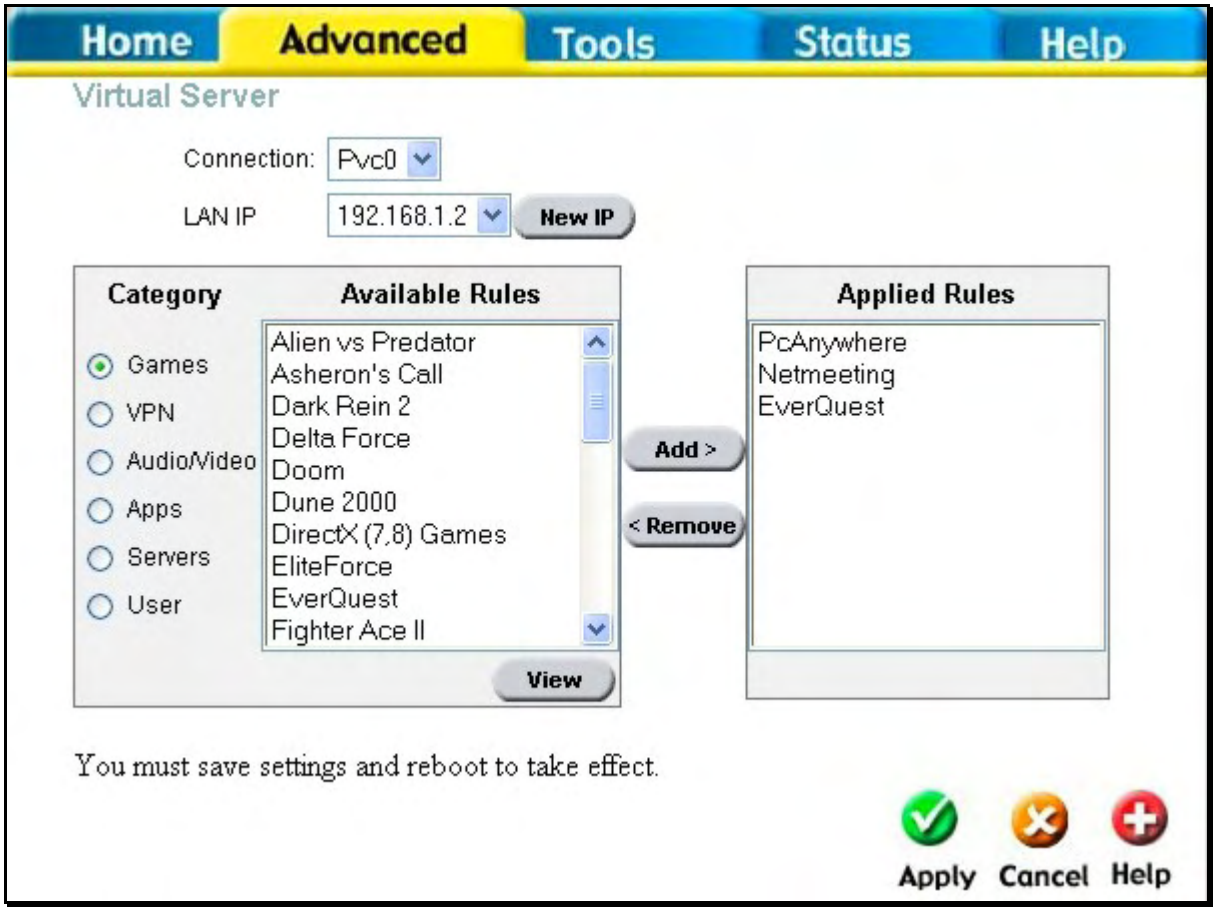
Use the **Virtual Server** window to set up single-port, trigger port or static-port range forwarding rules applied to inbound (WAN-to-LAN) traffic. The Virtual Server function allows remote users to access services on your LAN such as FTP for file transfers or SMTP and POP3 for e-mail. The DSL-2640T will accept remote requests for these services at your Global IP Address, using the specified TCP or UDP protocol and port number, and then redirect these requests to the server on your LAN with the LAN IP address you specify. Remember that the specified Private IP Address must be within the useable range of the subnet occupied by the Router.

UDP/TCP port redirection is used to direct inbound traffic to the specified servers or workstations on your private network. Port redirection can also be used to direct potentially hazardous packets to a proxy server outside your firewall. For example, you can configure the Router to direct HTTP packets to a designated HTTP server in the DMZ. You can define a set of instructions for a specific incoming port or for a range of incoming ports. Each set of instructions or rule is indexed and can be modified or deleted later as needed.

The Virtual Server options include a list of preconfigured rules (listed below) for commonly used protocols in the Virtual Server List. To enable a preconfigured rule, click the selection box for the rule you want to enable and click the **Apply** button.

Note

Use the LAN Clients window to select eligible IP addresses before configuring forwarding rules. See LAN Clients below.



Virtual Server window

There are many different pre-configured rules available for specific functions such as Internet gaming, VPN, streaming and interactive multi-media, standard TCP/IP protocols, reserved ports, p2p, network management applications, and so on.

You may also create customized rules to manage TCP/UDP ports. The pre-configured rules include those listed in the table here:

Category	Available Rules
Games:	Alien vs. Predator, Asheron's Call, Dark Rein 2, Delta Force, Doom, Dune 2000, DirectX (7.8) Games, EliteForce, EverQuest, Fighter Ace II, Half Life, Heretic II, Hexen II, Kali, Motorhead, MSN Gaming Zone, Myth: The Fallen Lords, Need for Speed Porsche, Need for Speed 3, Outlaws, Rainbow 6, Rogue Spear, Starcraft, Tiberian Sun, Ultima, Unreal Tournament, Quake 3 Server, Quake 2 Server, and Unreal Server.
VPN	IPSec (L2TP) and PPTP
Audio/Video	Net2Phone, Netmeeting, and QuickTime 4 Server
Applications	VNC, Win2k Terminal, PC Anywhere, Netbios, RemoteAnything, Radmin, LapLink, CarbonCopy, and Gnutella.
Servers	Web, FTP, Telnet, DNS, LDAP, NNTP, SMTP, POP 2, POP 3, IMAP, IRC, Lotus, and Remotely Possible.
User	Use this to set up custom TCP/UDP port rules.

To configure a new port-forwarding rule for any of the pre-configured rules, follow these steps:

1. Select the WAN connection you want to use for the new rule from the **Connection** pull-down menu.
2. Select a **LAN IP** from the available client IP addresses listed in the pull-down menu; or, create a **New IP** by clicking the button. This brings up the **LAN Clients** window (see next section).
3. Select the **Category** of the rule you are creating. The **Available Rules** for the category appear in a list.
4. Highlight to select the Available Rule you want to apply.
5. Click on the **Add>** button to place the rule in the **Applied Rules** list of port forwarding that are actively applied to the client

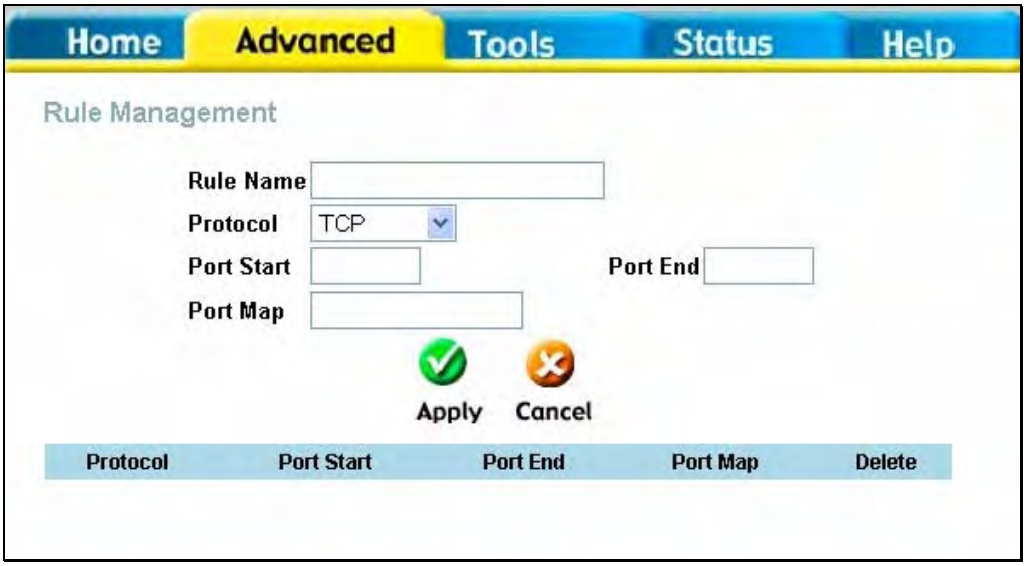
The Available Rules can be applied to a single client IP address. That is, it is not possible to use an applied rule for multiple IP addresses on the LAN.

Custom Forwarding Rules

The **User** category for port forwarding is used to set up customized port forwarding rules.

To set up custom TCP or UDP port forwarding rules, follow these steps:

1. Select the User category and click the **Add** button located below the Available Rules list. This will change the window to look like the window below.

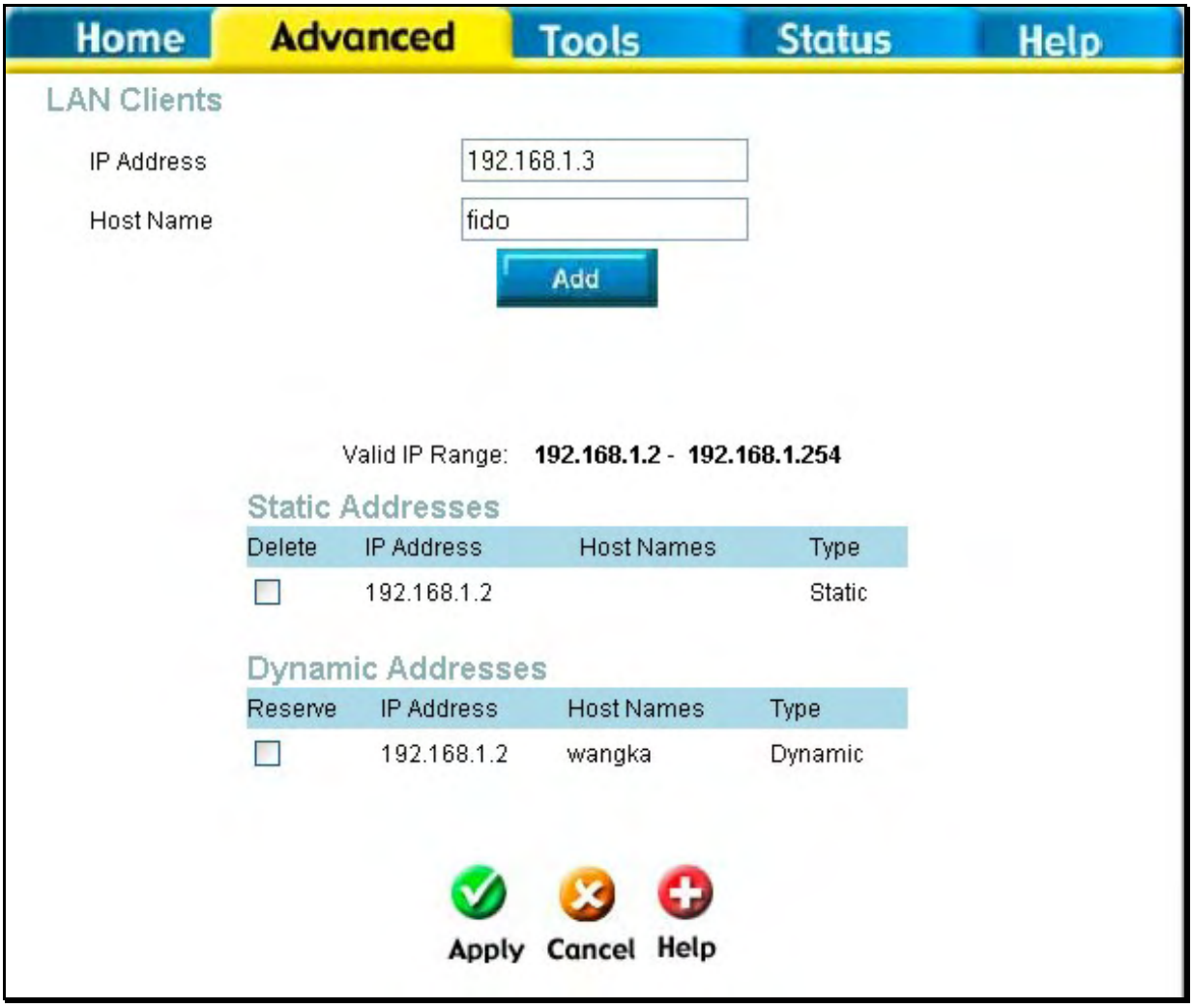


2. Type a **Rule Name** in the space provided.
3. Select the port **Protocol** from the pull-down menu - you may select *TCP*, *UDP* or both (*TCP/UDP*).
4. Configure a range of ports for forwarding. Type the lowest numbered port in the range in the **Port Start** space. Type the highest numbered port in the **Port End** space. For a single port, just enter the same number in both spaces.
5. Type a number for the **Port Map** in the space provided.
6. Click the **Apply** button to create the new rule. The new rule will appear listed in the table of custom port forwarding rules.

LAN Clients

The **LAN Clients** window is used when establishing port forwarding rules in the **Virtual Server** and **Filters** windows. This window can be accessed directly by clicking on the **LAN Clients** button in the **Advanced** tab. In order to use these advanced features it is necessary to have IP addresses available for configuration. If there are no IP addresses listed in the **LAN Clients** window, you will not be able to access the **Virtual Server** window.

Use the **LAN Clients** window to add or delete static IP addresses for the advanced functions mentioned above, or to Reserve a Dynamically assigned IP address for an advanced function. Dynamically assigned IP addresses will only be listed if DHCP is enabled on the Router.



LAN Clients window

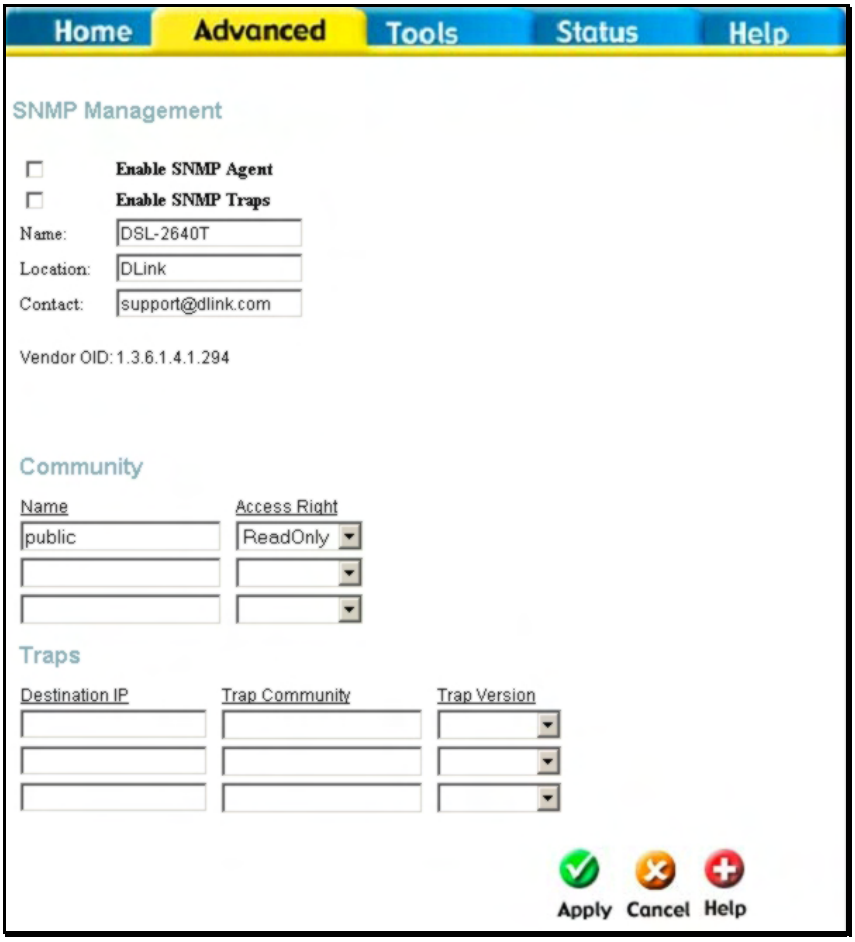
To add a static IP address to the list of available IP addresses, type an IP address that falls within the range a available IP addresses and click on the **Add** button. In the example above, available addresses range from 1.0.0.1 to 223.255.255.254. Any addresses added will appear in the list of **Static Addresses** available for advanced configuration.

To delete an IP address from the list of Static Addresses, click the **Delete** box for the address or addresses you want to eliminate and click on the **Apply** button.

Dynamically assigned IP addresses may be reserved so that the lease does not expire for the LAN IP address. Click the Reserve box for the address or addresses you want to reserve and click the **Apply** button. These addresses will become Static IP addresses and will no longer be available for DHCP assignment.

SNMP

Simple Network Management Protocol is a standard for internetwork and intranetwork management.



SNMP Management window

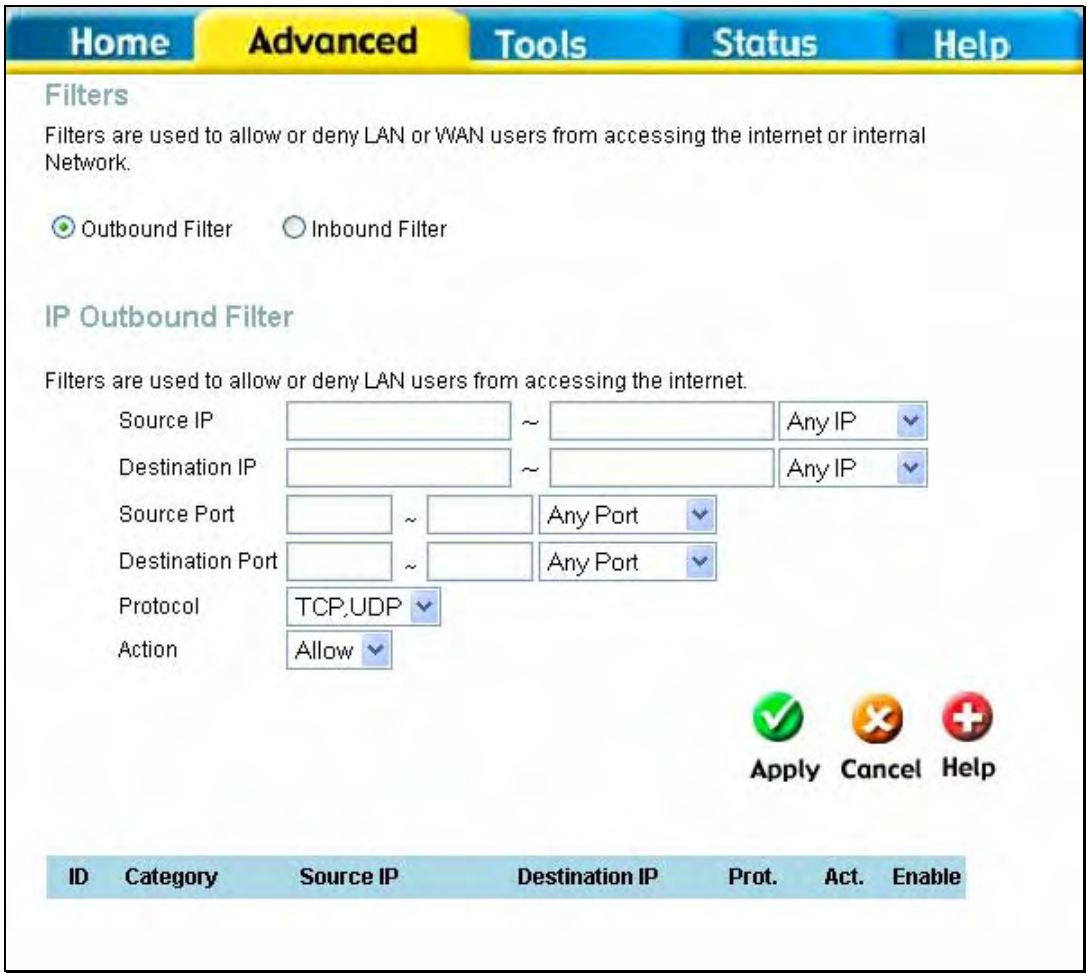
Configure these parameters for SNMP on the Router:

SNMP Category	Parameters
SNMP Management	This is used to enable or disable SNMP Agent and SNMP Traps or edit client SNMP Name, Location and Contact. • Enable SNMP Agent: Click to select enable or disable SNMP Agent. • Enable SNMP Traps: Click to select enable or disable SNMP Traps.
Community	Use this edit client community for server SNMP access. • Name: Edit community Name. • Access Right: Access Right may choose ReadOnly or ReadWrite.
Traps	The management agent can send an event notification to the management system to identify the occurrence of conditions such as threshold that exceeds a predetermined value. • **Destination IP:** Insert destination IP address to launch trap message. • **Trap Community:** Insert Trap Community name. • **Trap Version:** Drop-down menu allows you to select SNMP v1 or SNMP v2c.

Filters

Filter rules in the Router are put in place to allow or block specified traffic. The Filter Rules however can be used in a single direction to examine and then Allow or Deny traffic for Inbound (WAN to LAN) or Outbound (LAN to WAN) routed data. The rules are based on IP address and TCP/UDP port.

Configure the filter rules as desired and click the **Apply** button to create the rule. The newly created rule appears listed in the Outbound Filter List at the bottom of the window. The table below describes the various parameters that are configured for the filter rules.



Filters window

To modify any previously created filter rule, click on the note pad icon in the right hand column of the Filter List for the set you want to configure. Adjust the settings as desired and click the **Apply** button to put the new settings into effect.

First determine the direction of the traffic you want the rule to filter. To filter WAN to LAN traffic, select the **Inbound Filter** option. Any new Inbound Filter rules created will appear in the list. Likewise, should you to filter LAN to WAN traffic, create an **Outbound Filter** rule.

Note

The Service Filtering feature of the Firewall may interfere with ules configured in the Filters window. For example, FTP packets are not allowed through from the external network by default. See the Firewall section below for details.

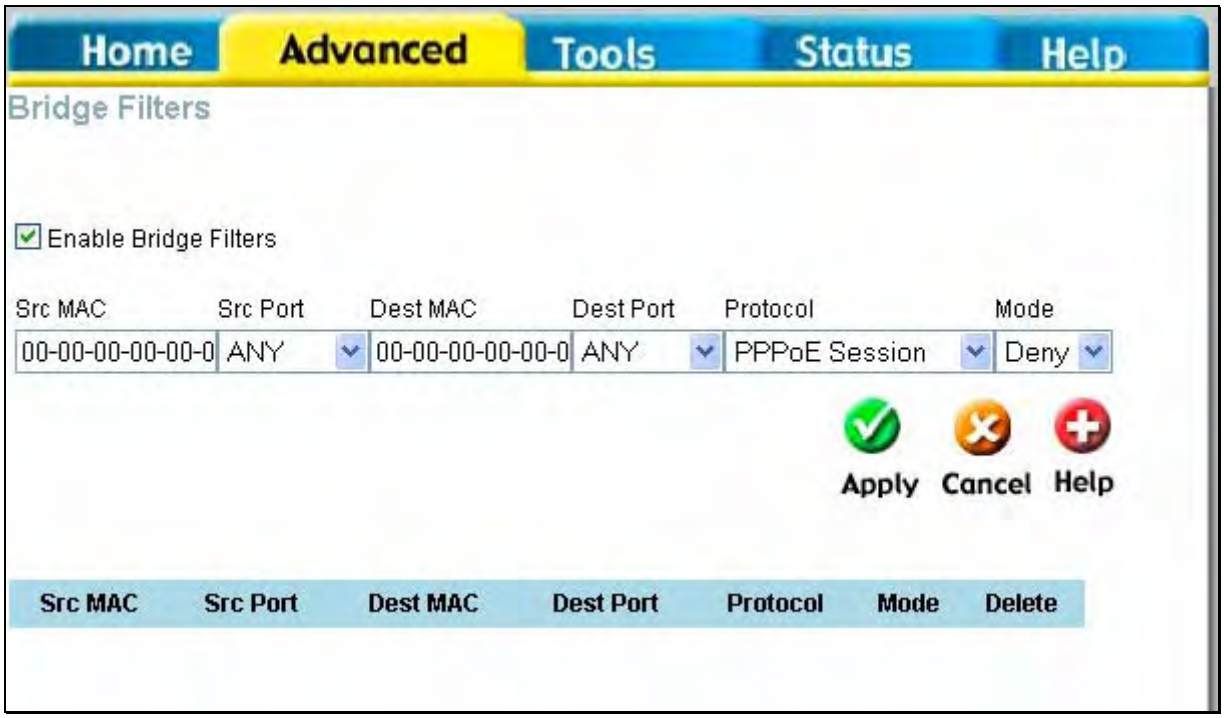
The parameters described in the table below are used to set up filter rules.

Click the **Apply** button to put the new rule into effect. Any filter rule configured in the menu will appear in the Filters List with the new settings. The Router must save the new settings and reboot before the new rules are applied.

Filters Parameter	Description
Source IP	For an Outbound Filter, this is the IP address or IP addresses on your LAN for which you are creating the filter rule. For an Inbound Filter, this is the IP address or IP addresses for which you are creating the filter rule. You can opt to indicate a *Single IP*, an *IP Range* or *Any IP* from the pull-down menu. Choosing Any IP will apply the rule to all WAN or all LAN IP addresses depending on which type of rule (Inbound or Outbound) is being configured.
Destination IP	Where the Destination IP address resides also depends on if you are configuring an Inbound or Outbound filter rule. You can opt to indicate a *Single IP*, an *IP Range* or *Any IP* from the pull-down menu.
Source Port	The Source Port is the TCP/UDP port on either the LAN or WAN depending on if you are configuring an Outbound or Inbound Filter rule. Select one of the following options from the pull-down menu to define *Any Port, Single Port*, *Port Range* or *Safe Range* (ports above 1024).
Destination Port	The Destination Port is the TCP/UDP port on either the LAN or WAN depending on if you are configuring an Outbound or Inbound Filter rule. Select one of the following options from the pull-down menu to define a *Any Port, Single Port*, *Port Range* or *Safe Range* (ports above 1024).
Protocol	Select the transport protocol (*TCP*, *UDP* or *TCP/UDP*) that will be used for the filter rule.
Action	Select to *Allow* or *Deny* transport of the data packets according to the criteria defined in the rule. Packets that are allowed are routed to their destination; packets that are denied are blocked.

Bridge Filters

Bridge filters are used to block or allow various types of packets through the WAN interface. This may be done for security or to improve network efficiency. The rules are configured for individual devices based on MAC address. Filter rules can be set up for source, destination or both. You can set up filter rules and disable the entire set of rules without loosing the rules that have been configured.



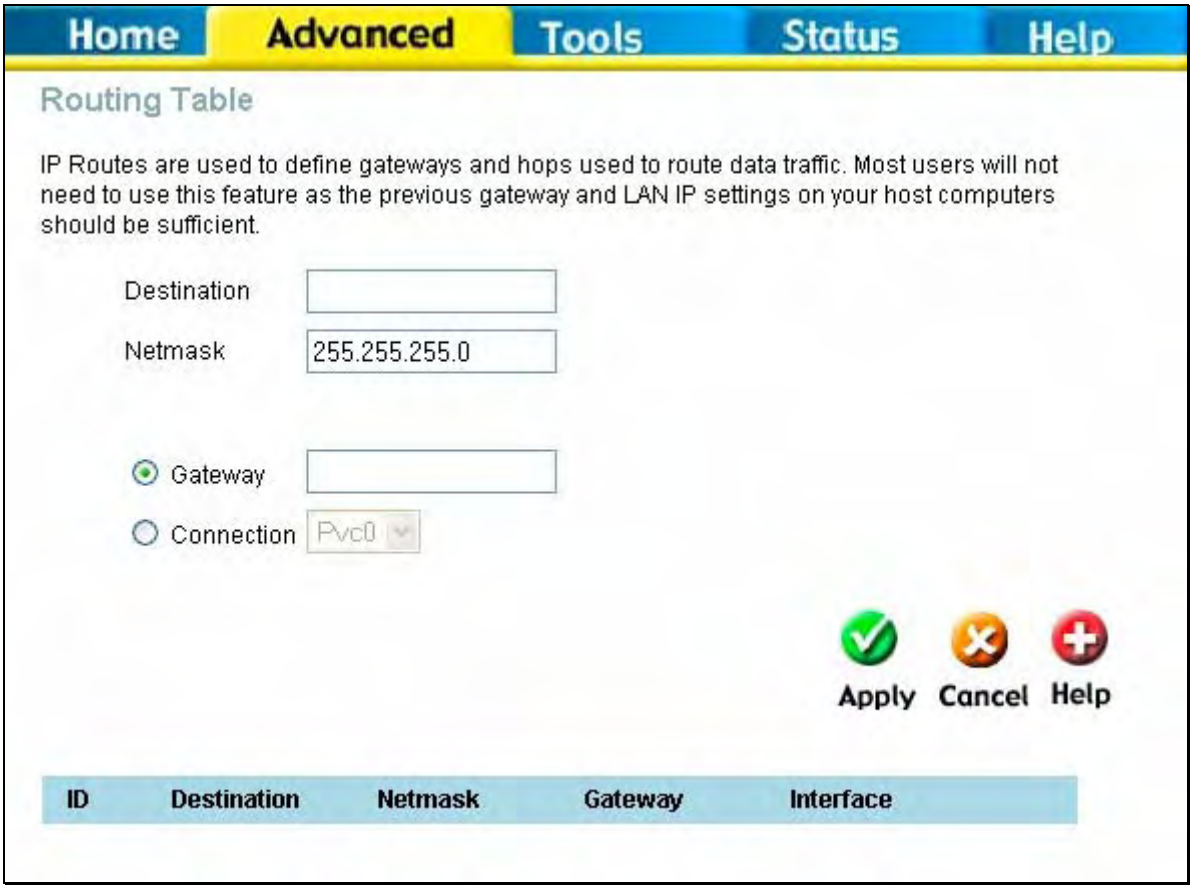
Bridge Filters window

To add a bridge filter rule, check **Enable Bridge Filters**, type in a Source MAC, a Destination MAC or both in the entry fields, you may opt to limit filtering to only the Ethernet, and click the **Apply** button. To remove a bridge filter from the table in the bottom half of the window, click the corresponding trashcan icon. Remember to save the configuration changes.

The protocols that may be specifically allowed or denied to pass through the WAN interface are the following: *IPv4*, *IPv6, RARP, PPPoE Discovery* and *PPPoE Session.*

Static Routing

Use Static Routing to specify a route used for data traffic within your Ethernet LAN or to route data on the WAN. This is used to specify that all packets destined for a particular network or subnet use a predetermined gateway.



Routing Table window

To add a static route to a specific destination IP on the local network, enter a **Destination** IP address, **Netmask**, then click the **Gateway** radio button and type in the Gateway's IP address. Click **Apply** to enter the new static route in the table below. The route becomes active immediately upon creation.

To add a static route to a specific destination IP on the WAN, click the Connection radio button and choose a connection from the pull-down menu, then enter a **Destination** IP address and **Netmask**. Click **Apply** to enter the new static route in the table below. The route becomes active immediately upon creation

To remove a static route from the table in the bottom half of the window, choose to Delete it from the table and click the **Apply** button. Remember to save the configuration changes.

DMZ

Firewalls may conflict with certain interactive applications such as video conferencing or playing Internet video games. For these applications, a firewall bypass can be set up using a DMZ IP address. The DMZ IP address is a "visible" address and does not benefit from the full protection of the firewall function. Therefore it is advisable that other security precautions be enabled to protect the other computers and devices on the LAN. It may be wise to use isolate the device with the DMZ IP address from the rest of the LAN.

For example, if you want to use video conferencing and still use a firewall, you can use the DMZ IP address function. In this case, you must have a PC or server through which video conferencing will take place. The IP address of this PC or server will then be the DMZ IP address. You can designate the server's IP address as the DMZ by typing in the IP address in the **IP Address** space provided and then enabling its status by clicking the **Enabled** radio button and then click **Apply**.

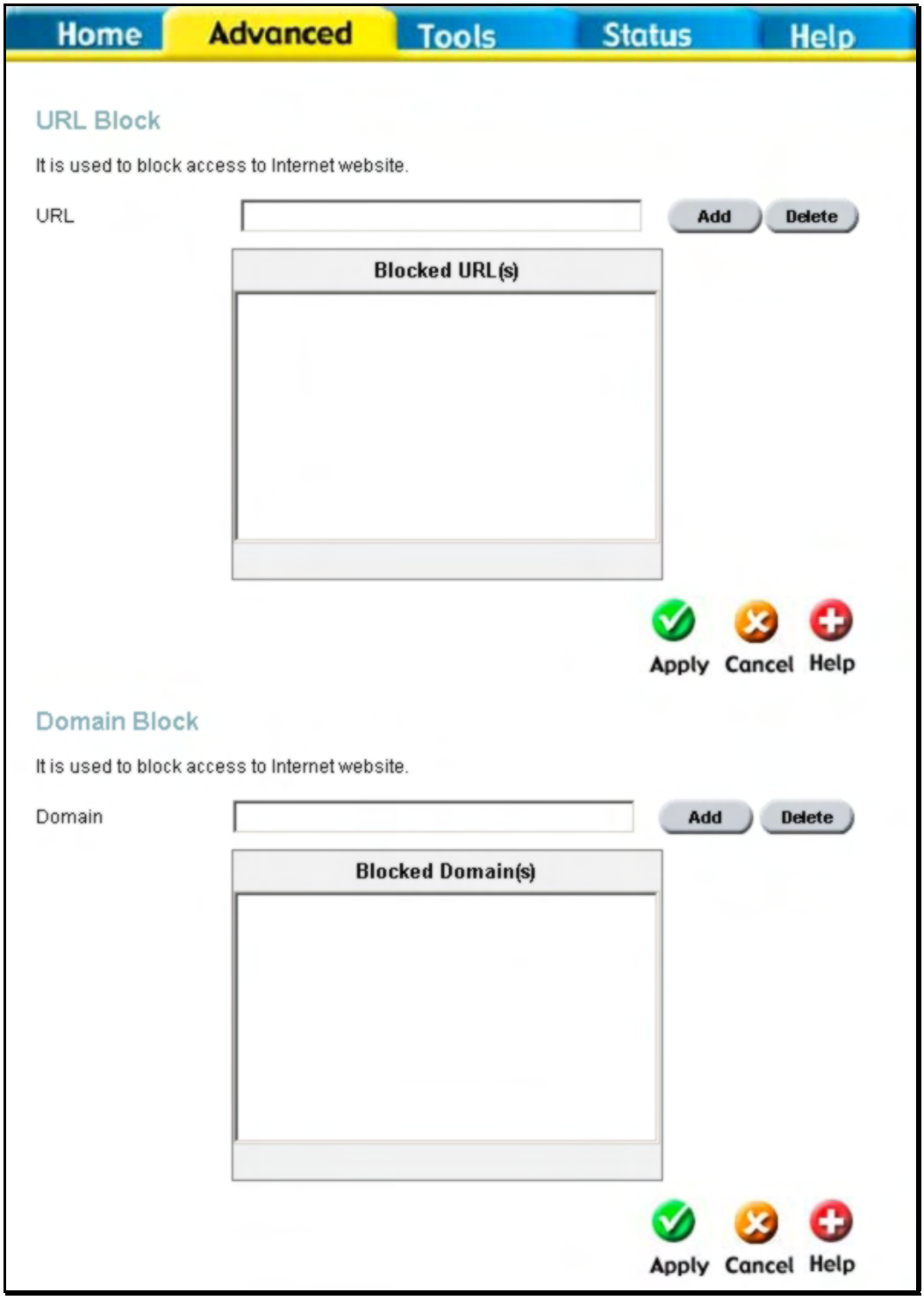
For the system that uses the DMZ IP address, you may want to manually assign an IP address to it and adjust your DHCP server addresses so that the DMZ IP address is not included in the DHCP server range. This way you avoid possible IP address problems if you reboot the DMZ system.

DMZ menu

To designate a DMZ IP address, select the **Enabled** radio button, type in the **IP Address** of the server or device on your LAN, and click the **Apply** button. To remove DMZ status from the designated IP address, select the Disabled radio button and click Apply. It will be necessary to save the settings and reboot the Router before the DMZ is activated.

Parental Control

Use Parental Controls to deny access to specified websites or websites containing specified words in the URL.



Parental Control menu

URL Blocking

URL or Uniform Resource Locator is a specially formatted text string that uniquely defines an Internet website. This window will allow users to block computers on the LAN from accessing certain URLs. This may be accomplished by simply entering the URL to be blocked in the **URL Address** field. The user may also use this field to block certain websites by entering a keyword into the **URL Address** field. So, if any website's URL contains this word, it will automatically be denied access to users on the LAN.

For example, if you wish to block users from accessing shopping websites, enter the keyword "shopping into the URL Address field. Then website having "shopping" in their URL (such as http://www.yahoo.com/shopping/stores.html or http://www.msn/search/shopping-spree.html) will be denied from computers on the LAN. This feature may be beneficial to parents wanting to stop their kids from accessing certain websites or for companies who want their employees to stop surfing the Internet on company time.

To configure this screen for URL blocking, enter the website's address or a keyword into the **URL** field and click **Add** button, then click **Apply** to save this configuration into the Routers memory. Configured URL blocking entries will be displayed in the **Blocked URLs** List at the bottom of the screen. To remove a Blocked URL entry in the list, click on the entry and click the **Delete** button.

Domain Blocking

Domain blocking is a method of denying computers on the LAN access to specific domains on the Internet.

To configure this screen for URL blocking, enter the website's address into the **Domain** field and click **Add** button, then click **Apply** to save this configuration into the Routers memory. Configured Domain blocking entries will be displayed in the **Blocked Domains** List at the bottom of the screen. To remove a Blocked Domain entry in the list, click on the entry and click the **Delete** button.

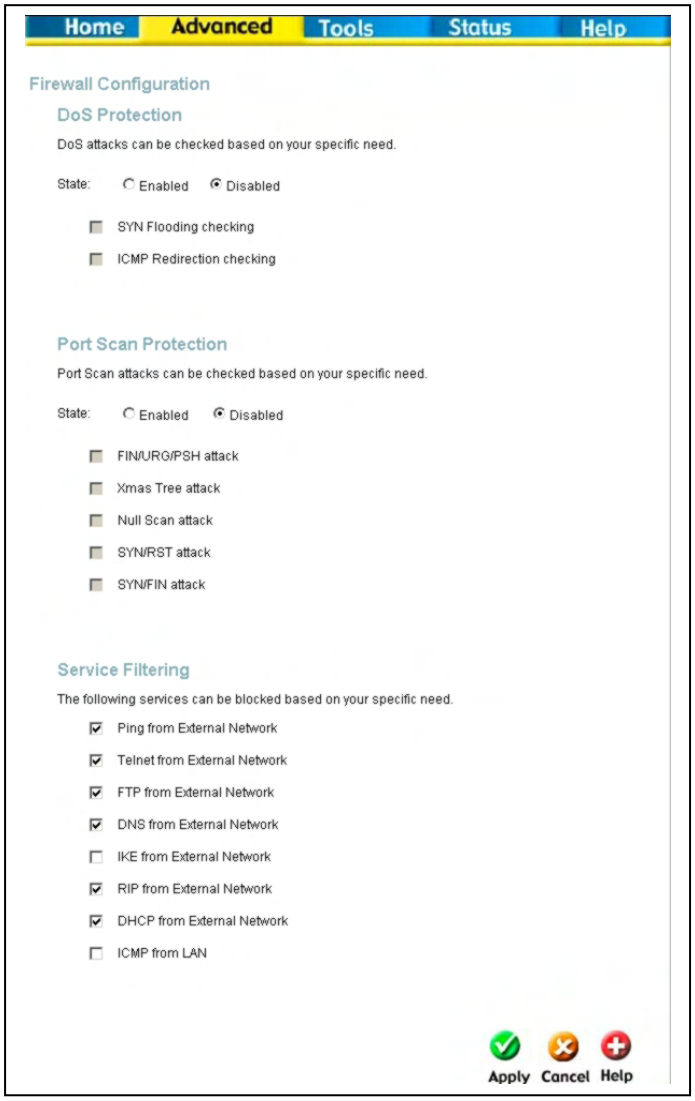
Firewall

The **Firewall Configuration** window allows the Router to enforce specific predefined policies intended to protect against certain common types of attacks. There are two general types of protection (DoS, Port Scan) that can be enabled on the Router, as well as filtering for specific packet types sometimes used by hackers.

You can choose to enable or disable protection against a customized basket of attack and scan types. To use **DoS Protection** or **Port Scan Protection**, select the **State** Enabled radio button for the protection type and click in the selection boxes for the various types of protection listed under each.

Note

Service Filtering may interfere with other configurations such as DHCP Relay or Remote Management via Telnet.



Firewall Configuration menu

When DoS, Port Scan, or Service Filtering Protection is enabled, it will create a firewall policy to protect your network against the following:

Dos Protection	Port Scan Protection	Service Filtering
• SYN Flood check • ICMP Redirection check	• FIN/URG/PSH attack • Xmas Tree Scan • Null Scan attack • SYN/RST attack • SYN/FIN Scan	• Ping from WAN • Telnet from WAN • FTP from WAN • DNS from WAN • IKE from WAN • RIP from WAN • DHCP from WAN • ICMP from LAN

A DoS "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include: attempts to "flood" a network, thereby preventing legitimate network traffic, attempts to disrupt connections between two machines, thereby preventing access to a service, attempts to prevent a particular individual from accessing a service, or, attempts to disrupt service to a specific system or person.

Port scan protection is designed to block attempts to discover vulnerable ports or services that might be exploited in an attack from the WAN.

The Service Filtering options allow you to block FTP, Telnet response, Pings, etc, from the external network. Check the category you want to block to enable filtering of that type of packet.

When you have selected the desired Firewall policies, click the **Apply** button to enforce the policies. Remember to save any configuration changes.

RIP

The Router supports RIP v1 and RIP v2 used to share routing tables with other Layer 3 routing devices on your local network or remote LAN.

RIP System Wide Configuration menu

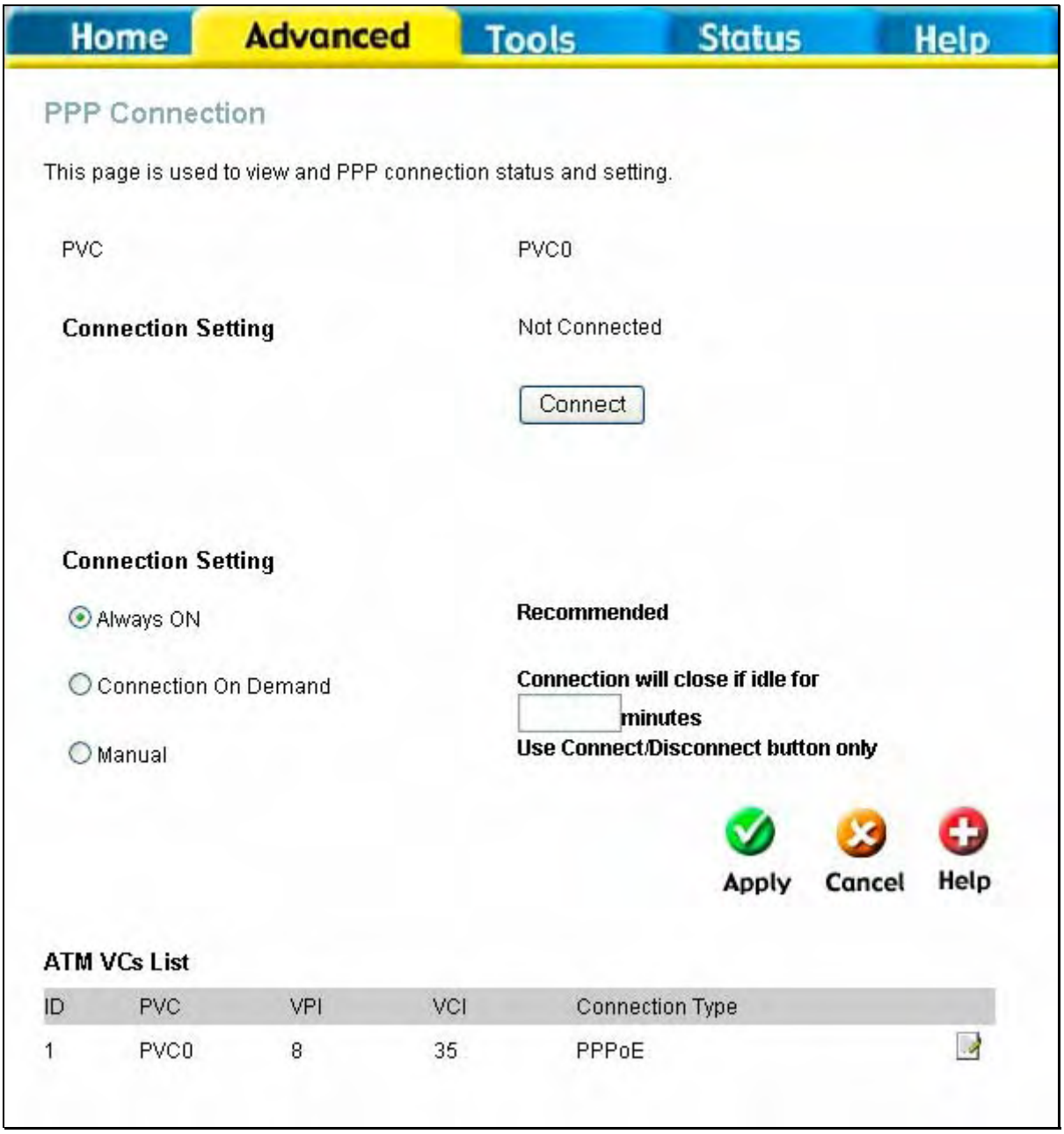
To enable RIP, select *Enabled* from the **RIP** pull-down menu, select the **Protocol** (*RIPv1* and *RIPv1 Compatible*) and **Direction** (*In*, *Out*, or *Both*), and click **Apply**.

The RIPv1 Compatible option will transmit RIPv2 broadcast packets and receive both RIP v1 and RIP v2 packets.

The direction configuration refers to the RIP request. Select In to allow RIP requests from other devices. Select Out to instruct the Router to make RIP requests for routing tables from other devices. Select *Both* to share routing tables in both directions.

PPP

When the WAN connection is configured for either PPPoA or PPPoE, you can configure the Router's PPP session to remain on all the time, or to disconnect after some period of no activity. You may also choose to instruct the Router to connect each time you want to access the WAN or the Internet.



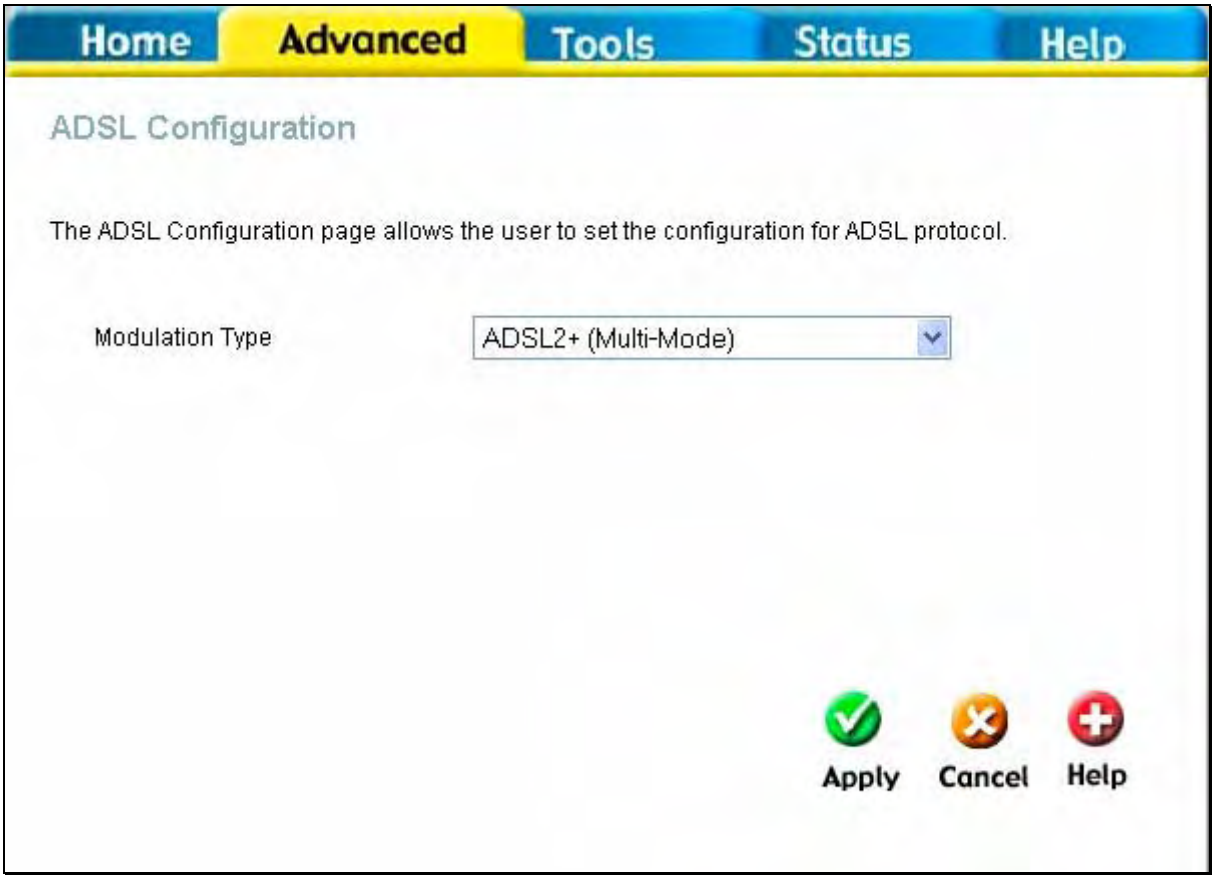
PPP Connection menu

If you want the Internet or WAN connection to be available any time a host on your LAN requests access, select the **Always On** option.

If your ISP account is billed according to the amount of time the Router is connected, choose the **Connection On Demand** option. You can configure an idle time in minutes to disconnect the PPP connection after a period of inactivity. This will discontinue the PPP session and require a few seconds to reconnect when a host requests access to the WAN. Alternatively you can choose the **Manual** option and use the **Connect** button to initiate a PPP connection each time you want to use the Router to access the WAN. If you use the Manual option, you must return to this menu and click the **Disconnect** button to terminate the PPP session.

ADSL

The **ADSL Configuration** window allows the user to set the configuration for ADSL protocols. For most ADSL accounts the default settings *ADSL2+(Multi-mode)* will work. This configuration works with all ADSL implementations. If you have been given instructions to change the Modulation method used, select the desired option from the **Modulation Type** drop-down menu and click the **Apply** button.

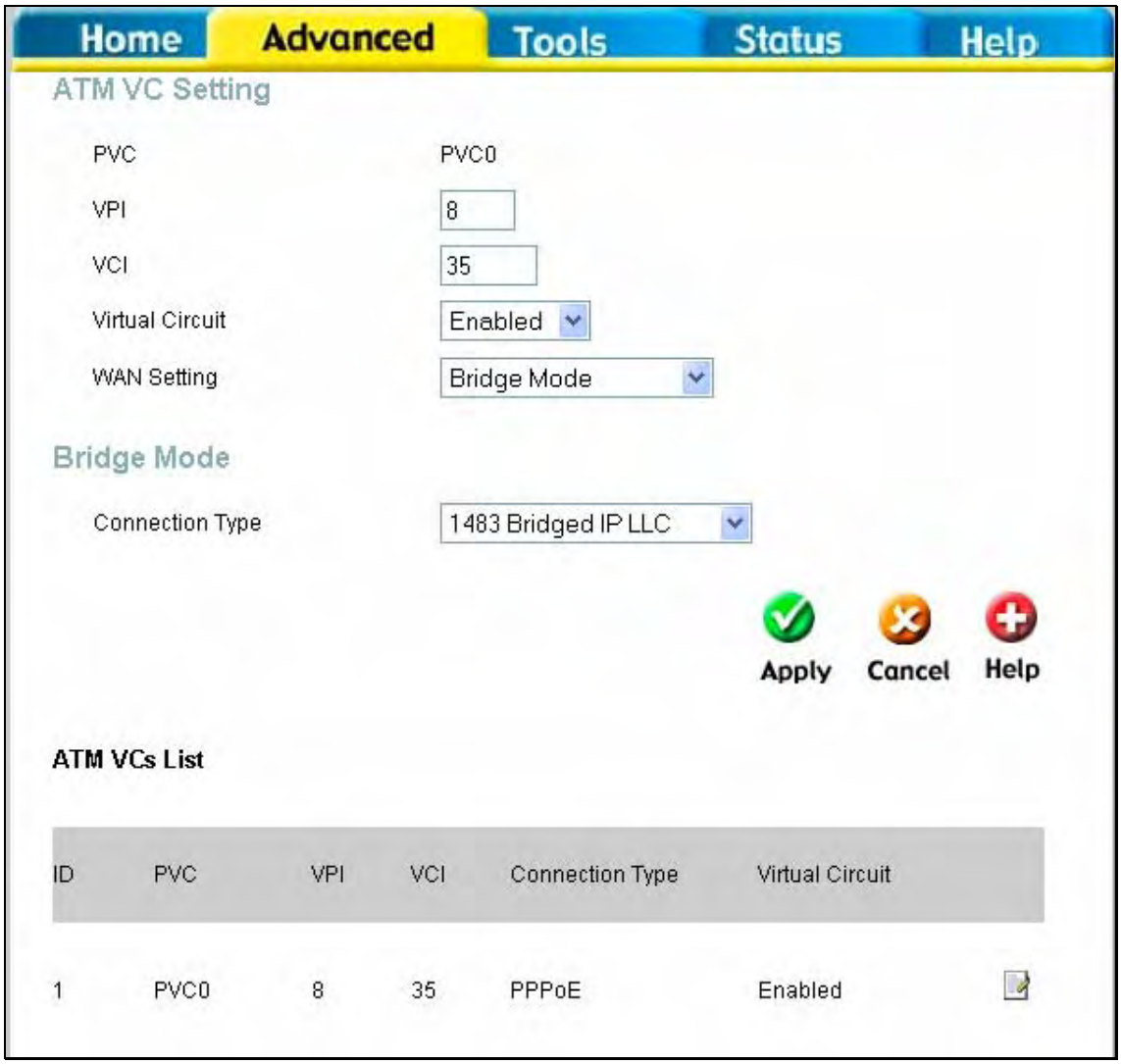


ADSL Configuration menu

ATM VCC

The **ATM VC Setting** window is used to configure the WAN connection. If you are using multiple PVCs, you can change the configuration of any PVC in this window. To create new or additional PVCs, read the section on Multiple PVCs on page 53.

This window can be used as an alternative to configure the same settings found on the WAN Settings window in the **Home** directory.



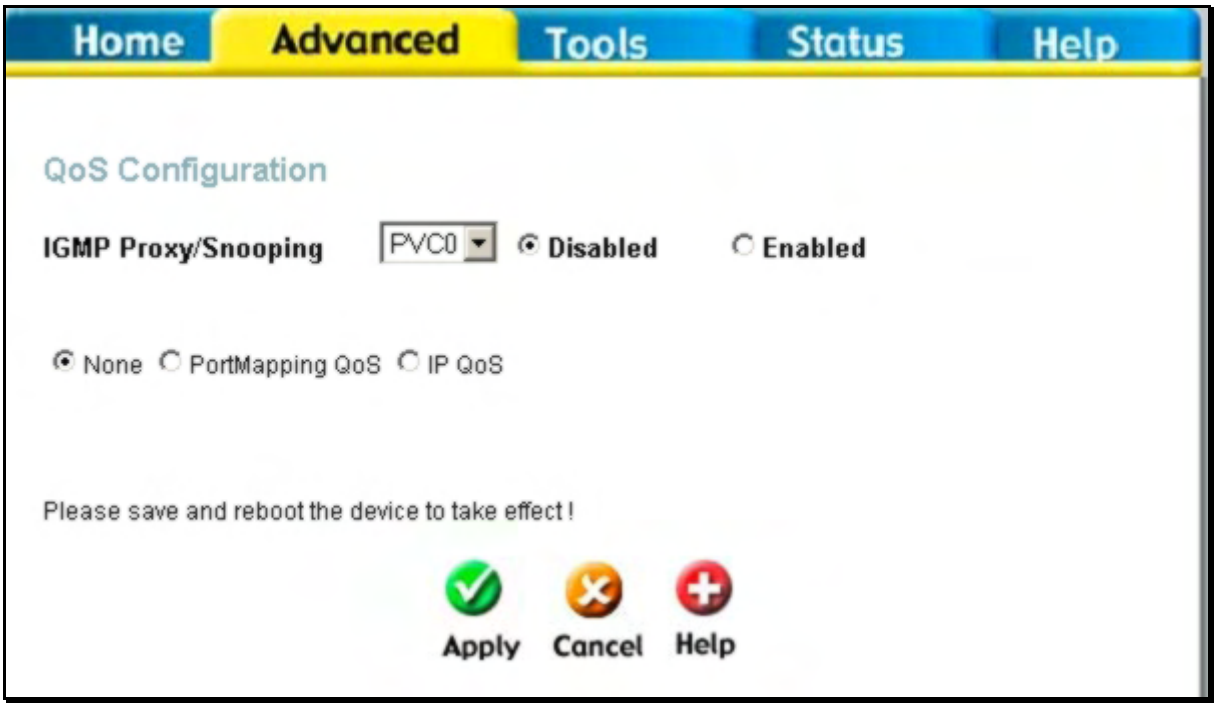
ATM VC Setting menu

To configure an existing PVC configuration set, click the corresponding notepad icon in the right-hand column of the ATM VCs List. The PVCs current settings appear above in the entry fields of the **ATM VC Setting** window. Configure the appropriate settings and click the **Apply** button to put the new settings into effect.

QOS

QoS or Quality of Service is used to assign priority for qualified traffic that passes through the Router's wired interfaces (LAN and WAN). The Router uses four priority levels with "1" being the highest priority while "4" is the lowest.

The **IGMP Proxy/Snooping** is Disabled by default. This setting will not allow IGMP (Internet Group Management Protocol) packets to be forwarded from the WAN to the LAN for the purpose of IGMP snooping, or from the LAN to the WAN to request multicast group membership (IGMP Proxy). IGMP is used to manage multicasting (streaming radio for example is a multicast), most users will not need to enable this. Some ISPs use IGMP to perform remote configuration for client devices, such as the Router. If unsure, check with the service provider. To enable IGMP service to the LAN interface, select Enabled and click the **Apply** button

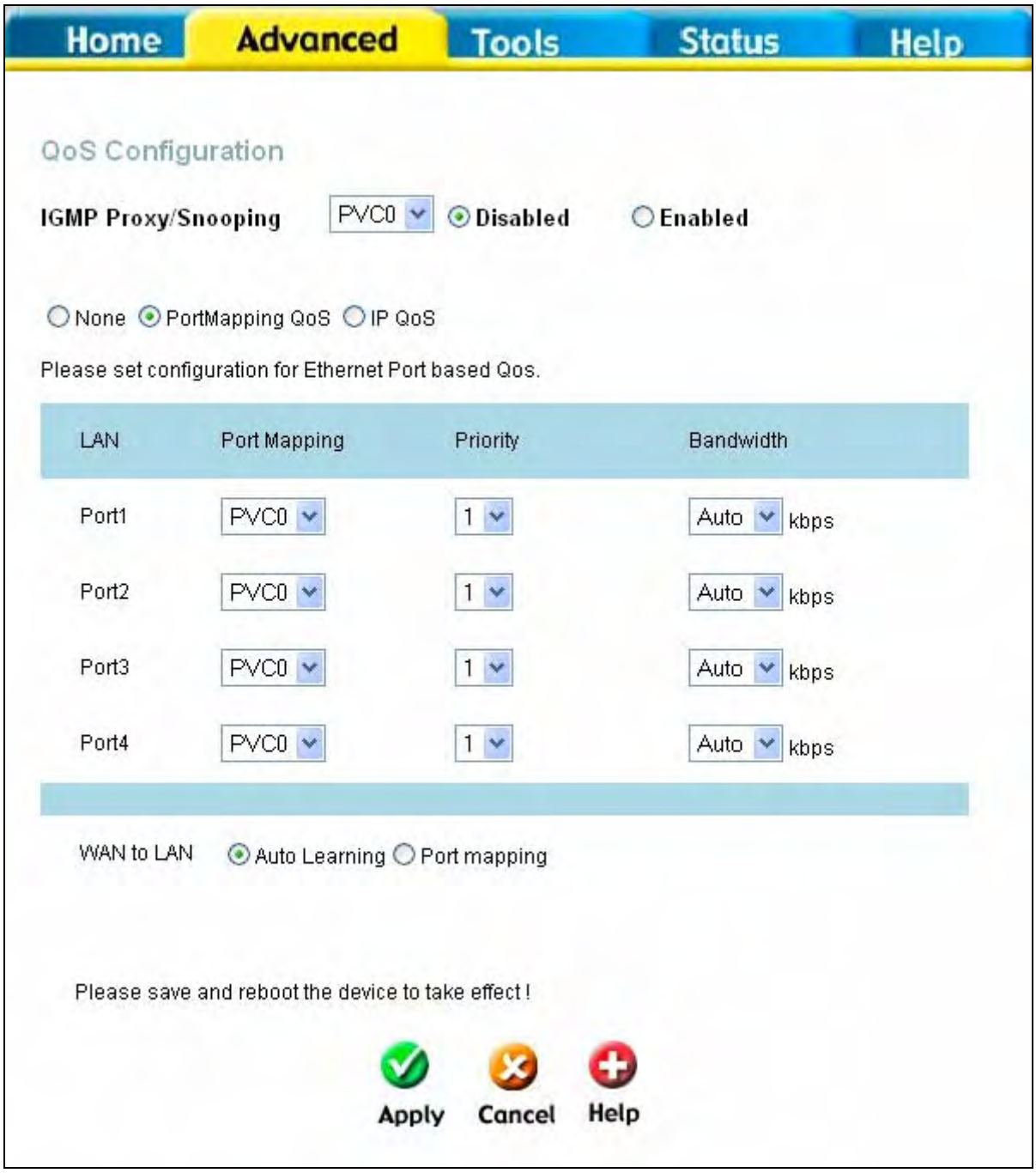


QoS Configuration menu

To set QoS for the router, first click the **PortMapping QoS** check box in the middle of the window. This will open the following window. Then select the PVC to associate with the corresponding port and choose a priority for this combination. The user may also enable IGMP Proxy/Snooping for any PVC at the top of the window by choosing the PVC from the pull-down menu and clicking the **Enabled** radio button and set a maximum **Bandwidth** in kbps from *Auto* to *64* using the drop-down menu. Click **Apply** to set the configuration.

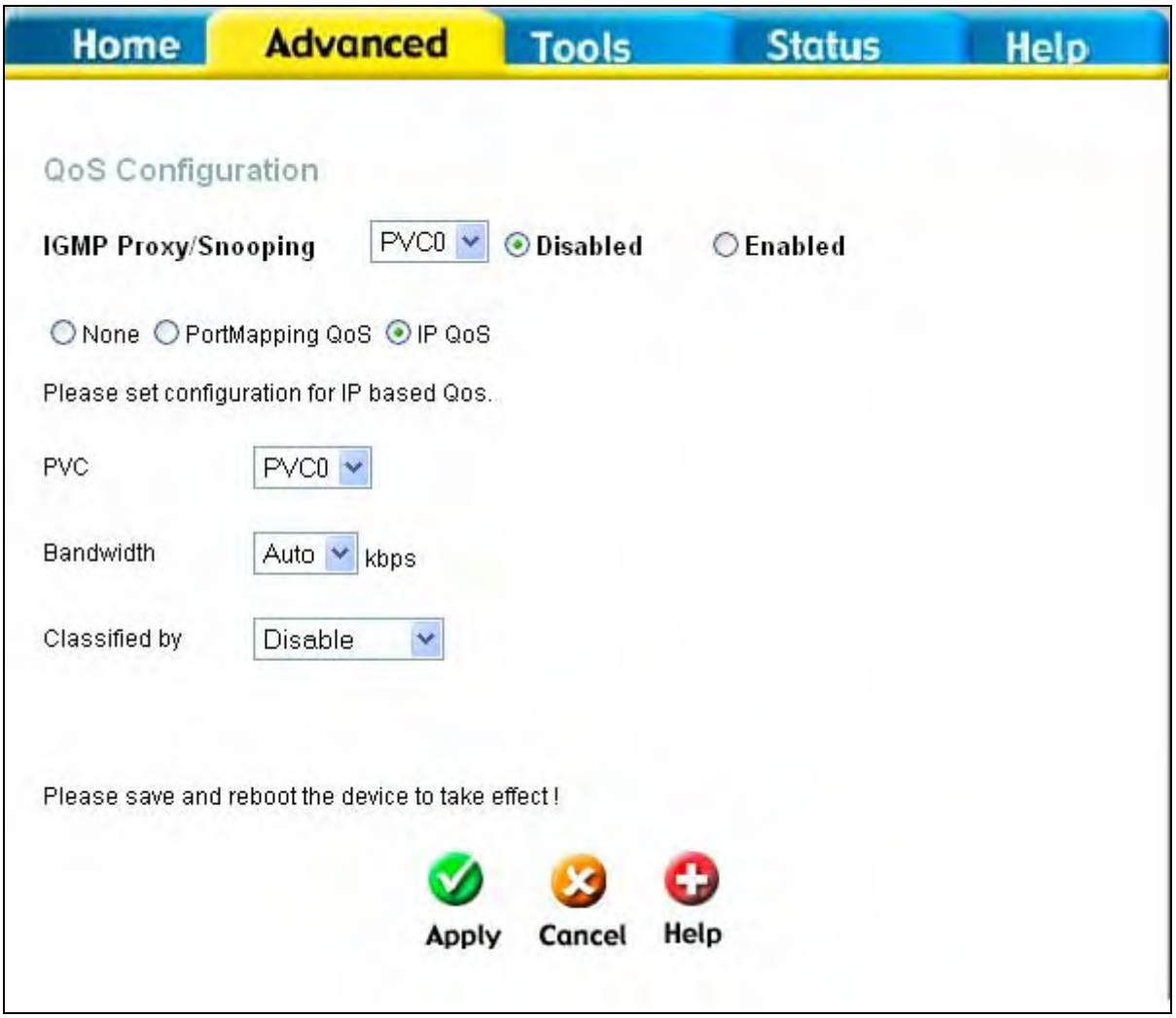
Note

QoS configured in the QoS menu applies only to data traffic on the Ethernet LAN and the WAN (ADSL) ports.



QoS Configuration window for Port Mapping QoS

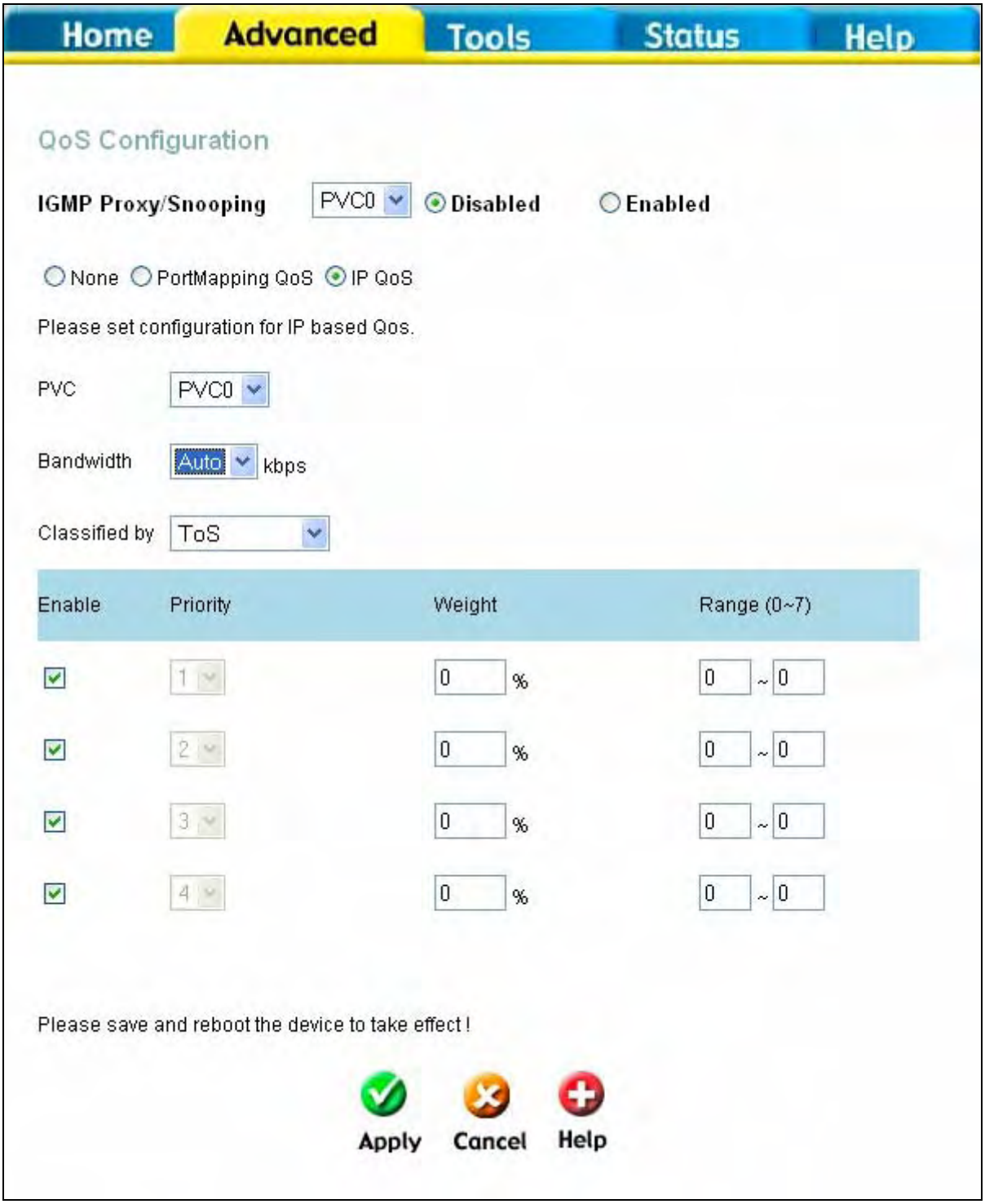
The Router can also be configured to use the QoS infomation contained in the header of IP packets. This will open the following window. To set IP QoS for the router, first click the **IP QoS** check box in the middle of the window. Then select the PVC to associate with the corresponding action and choose a maximum bandwidth and classification for this combination. Then select the classification type using the **Classified by** pull-down menu. The choices are *Disable*, *ToS*, *Application*, and *User Define*. Each choice will open the corresponding windows, shown following. The user may also enable IGMP Proxy/Snooping for each PVC at the top of the window by choosing the PVC from the pull-down menu and clicking the **Enabled** radio button and set a maximum **Bandwidth** in kbps from *Auto* to *64* using the drop-down menu. Click **Apply** to set the configuration.



QoS Configuration window IP QoS

If you select *Disable* in the **Classified by** drop-down menu, you can assign a maximum allowed bandwidth of between *64* kbps and *Auto* to each of the PVCs configured on the router.

Additional options become available when you select either *ToS*, *Application*, or *User Define* from the **Classified by** drop-down menu. Selecting *ToS* will display the following window.



QoS Configuration window IP QoS for ToS

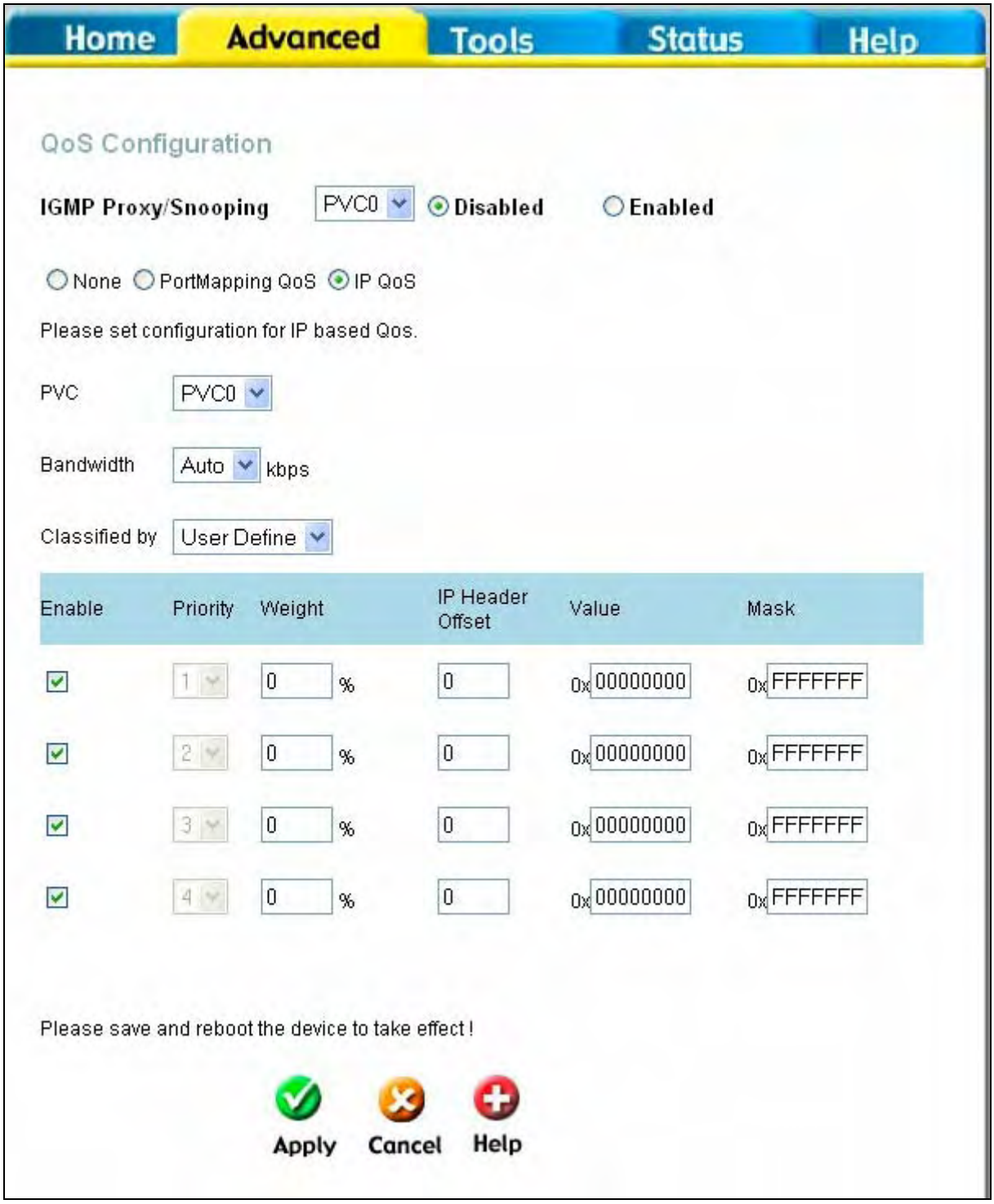
From this window you can input a Weight in percentage and a priority range that will determine the mechanism by which the four priority levels are "mapped". For example, if you assign 100% and a range of 0 to 7 to priority level 1, then the remaining priority levels (2 to 4) will only forward packets when priority level 1 is empty (when there are no packets to forward). Some experimentation may be necessary to achieve the optimum results with your particular ISP's connection.

If you select *Application* from the **Classified by** drop-down menu, the following window appears.

QoS Configuration window IP QoS for Application

On this window, you can select the mechanism by which the four priority queues are emptied by assigning a weight, in percentage terms, to each priority queue, and then assigning a packet type that can be associated with an application type. For example, if you assign a weight of 100% to Priority 1, with an application type of Voice, then the other 3 priority queues (2 to 4) will not be allowed to forward packets until all of the Voice packets have been sent from the priority 1 queue.

If you select *User Define* in the **Classified by** drop-down menu, the following window appears.

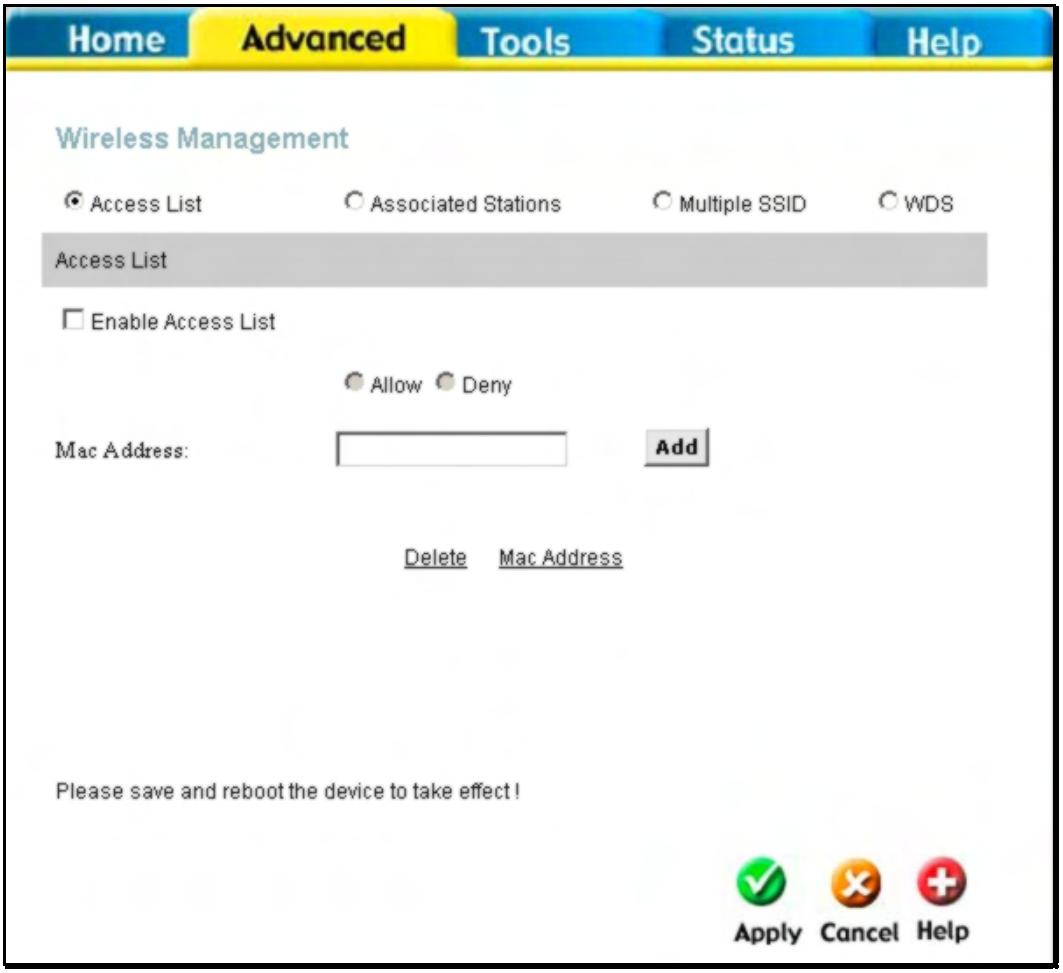


QoS Configuration window IP QoS for User Define

On this window, you can assign a weight, on a percentage basis, to each of the four priority queues. In addition, you can specify the number of bytes from the beginning of a given packet's IP header to set a pointer. From this pointer, you can then specify a Value (in hexadecimal) and a Mask (in hexadecimal) for the router to match when examining packets crossing the specified priority queue. It is recommended that you not enter a QoS scheme of this type unless you fully understand Offsets, pointers, masks, and IP headers or you are instructed to do so by your ISP.

Wireless Management

The Wireless Management menu includes separate menus for **Access List**, **Associated Stations** display, **Multiple SSID** operation and **WDS** (Wireless Distribution System). Click the appropriate radio button to view the menu for any of these Wireless Management menus.



Wireless Management - Access List menu

Access List

All computers are uniquely identified by their MAC (Media Access Control) address. The **Access List** menu is used to allow or deny computers access to the Router's Wireless interface based on their MAC address.

To enable the Access List, click to select the **Enable Access List** box and add MAC addresses to the list that will be allowed or denied access.

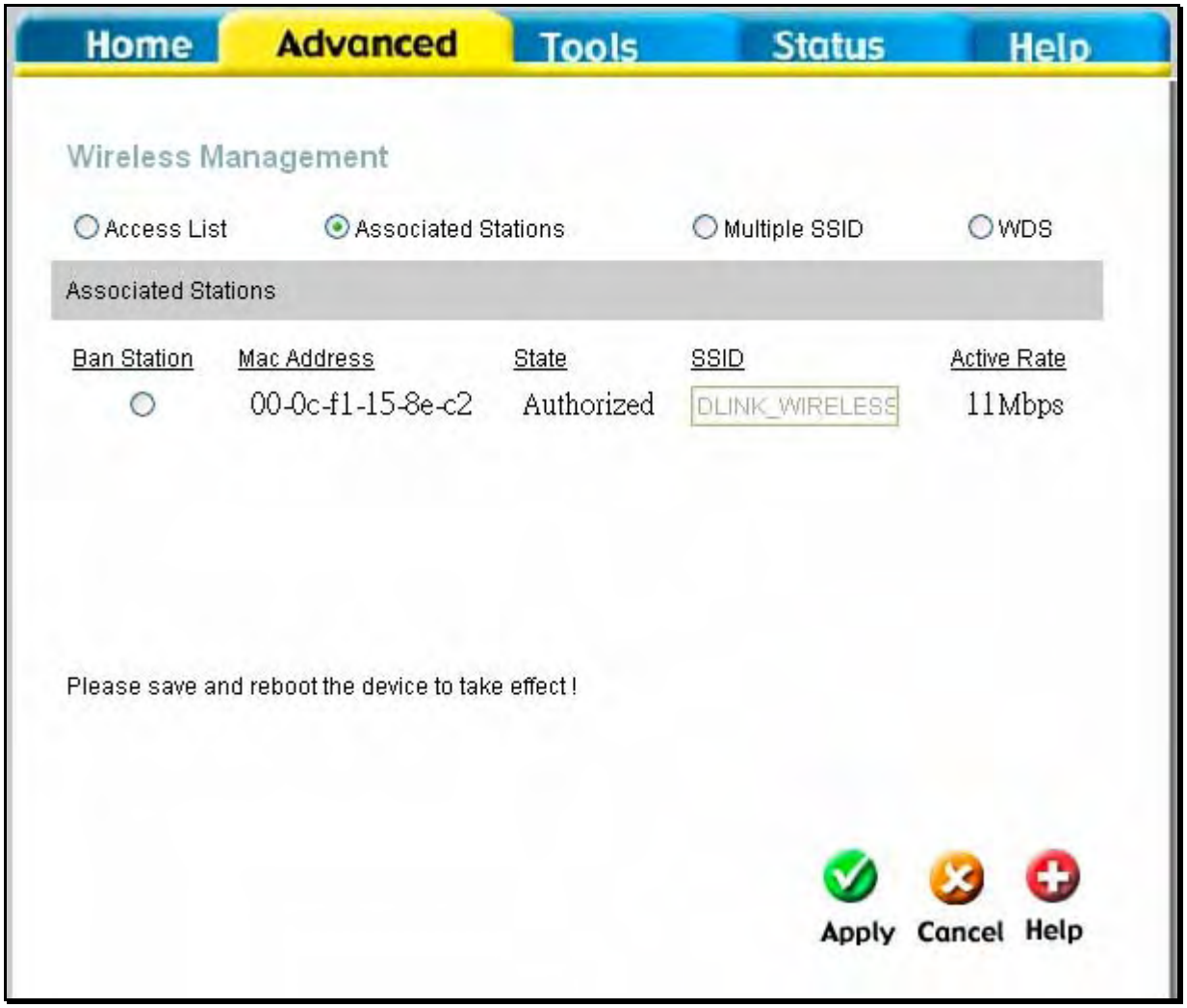
To add a MAC address to the list, enter the **MAC Address** in the entry field provided using the format **00-00-00-00-00-00**, select the radio button option to **Allow** or **Deny** access to the MAC address and click the **Add** button. The MAC address will appear listed below. To remove a MAC Address from the list, click the **Delete** radio button next to the MAC address.

All changes must be saved and the Router restarted for the Access List to be in effect.

The **Associated Stations** list can also be used to block access of any MAC address currently associated with the Acess Point (see next section).

Associated Stations

Use the Associated Stations list to view wireless stations currently associated with the access point.

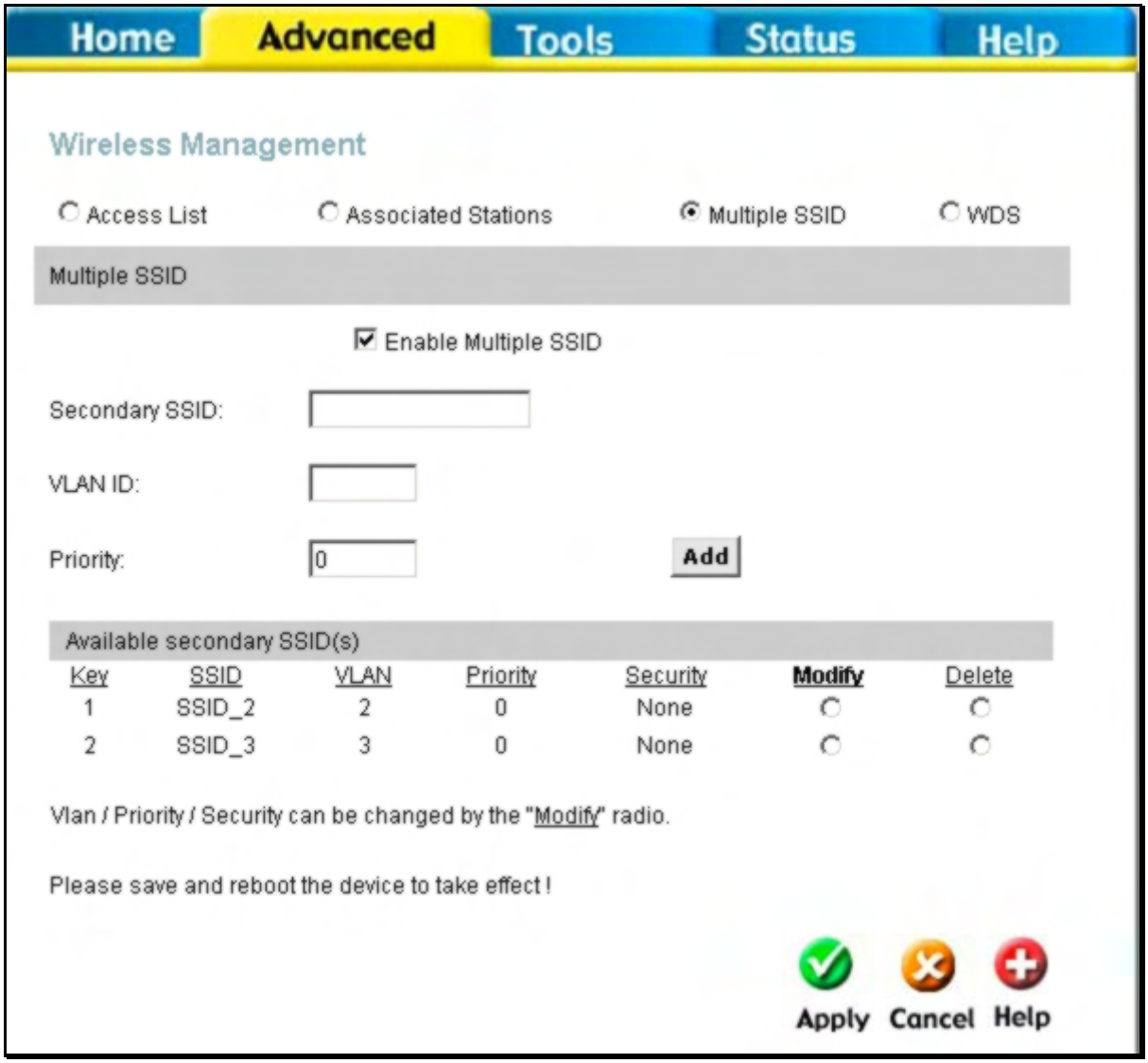


Wireless Management – Associated Stations display

The Associated Stations list displays the MAC address of stations currently associated with the Access Point. Any station on the list can be banned and have the MAC address added to the **Access List** of MAC addresses denied access. To deny access to any associated stations click the radio button for the MAC address you want to ban in the **Ban Station** column. Click **Apply** to add the banned station to the Access List (Denied) list. The change must be saved and the Router restarted before the banned station appears in the list of Denied stations on the Access List.

Multiple SSID

The access point in the Router supports use of multiple SSIDs. Up to 4 SSIDs may be used. Use the Multiple SSID menu to enable, create and configure additional SSIDs for your wireless network.



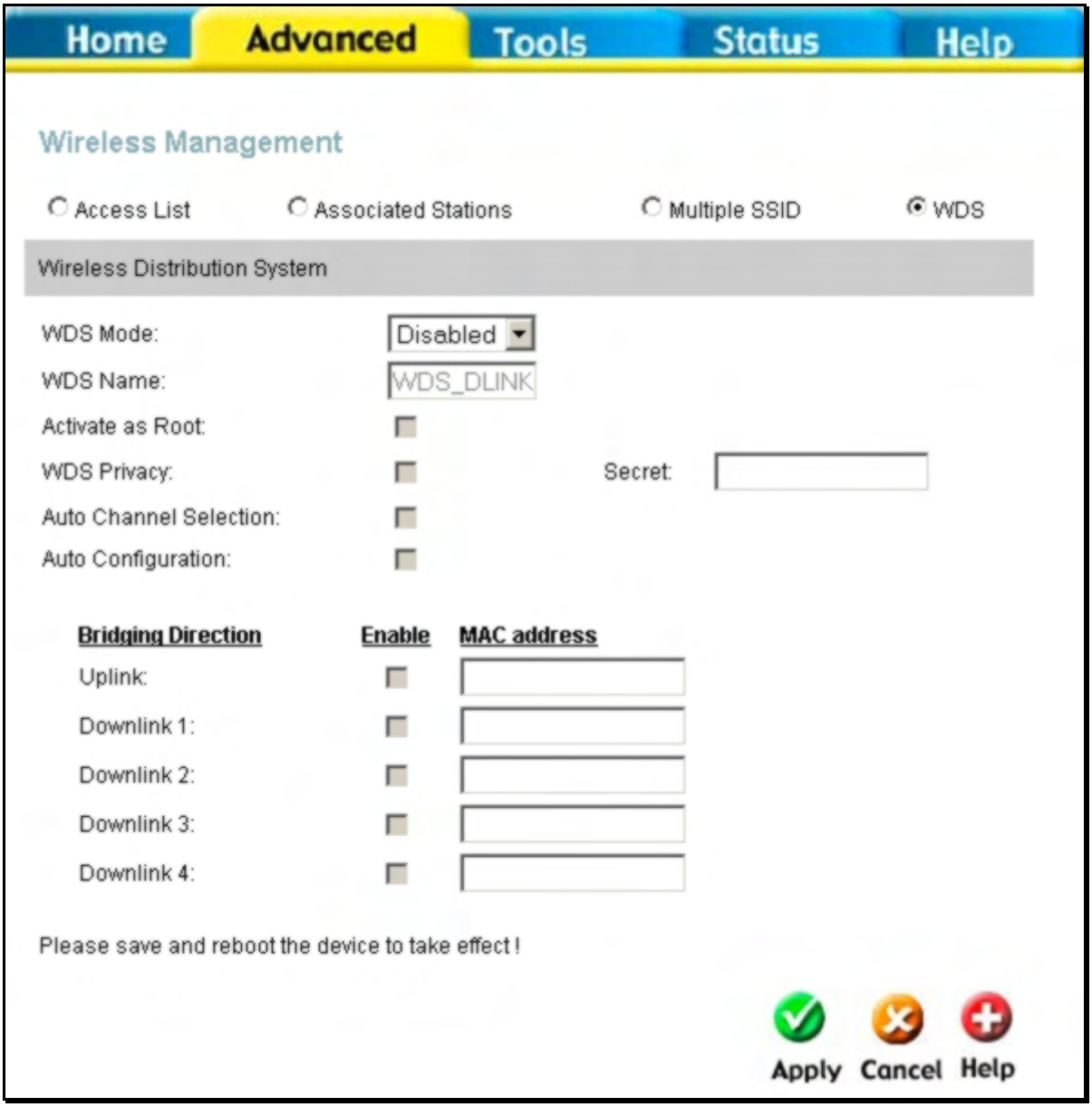
Wireless Management – Multiple SSID menu

To use multiple SSID operation, click to select the **Enable Multiple SSID** box. Multiple SSID must be enabled to create a new SSID configuration. After creating a secondary SSID, multiple SSID can be disabled by deselecting the Enable Multiple SSID box.

To add security settings to an existing secondary SSID, click the **Modify** radio button for that SSID and configure the security the same as configured in the general **Wireless Settings** menu (see page 28 for more information). To remove a secondary SSID, click the **Delete** radio button for the SSID to be removed.

Wireless Distribution System

The Router's access point supports Wireless Distribution System (WDS) to enable interconnection with other access points through the wireless network. WDS facilitates roaming between different access points and connectivity to the Ethernet and Internet. WDS is also used to connect two distant Ethernet LAN groups that may be be difficult or impractical to connect to each other with cable. The access point can perform different functions in the WDS depending on the mode that is chosen. To use WDS, first select the **WDS Mode** the access point will use from the pull-down menu, and configure the available parameters for the selected mode. See the table below for a description of the different modes and parameters used to configure the access point.



Wireless Management - WDS menu

When WDS is enabled, the Router's access point will operate in one of three modes, **Bridge** mode, **Repeater** mode or **Crude** mode. Use the table below as a guide to how each mode functions in the WDS.

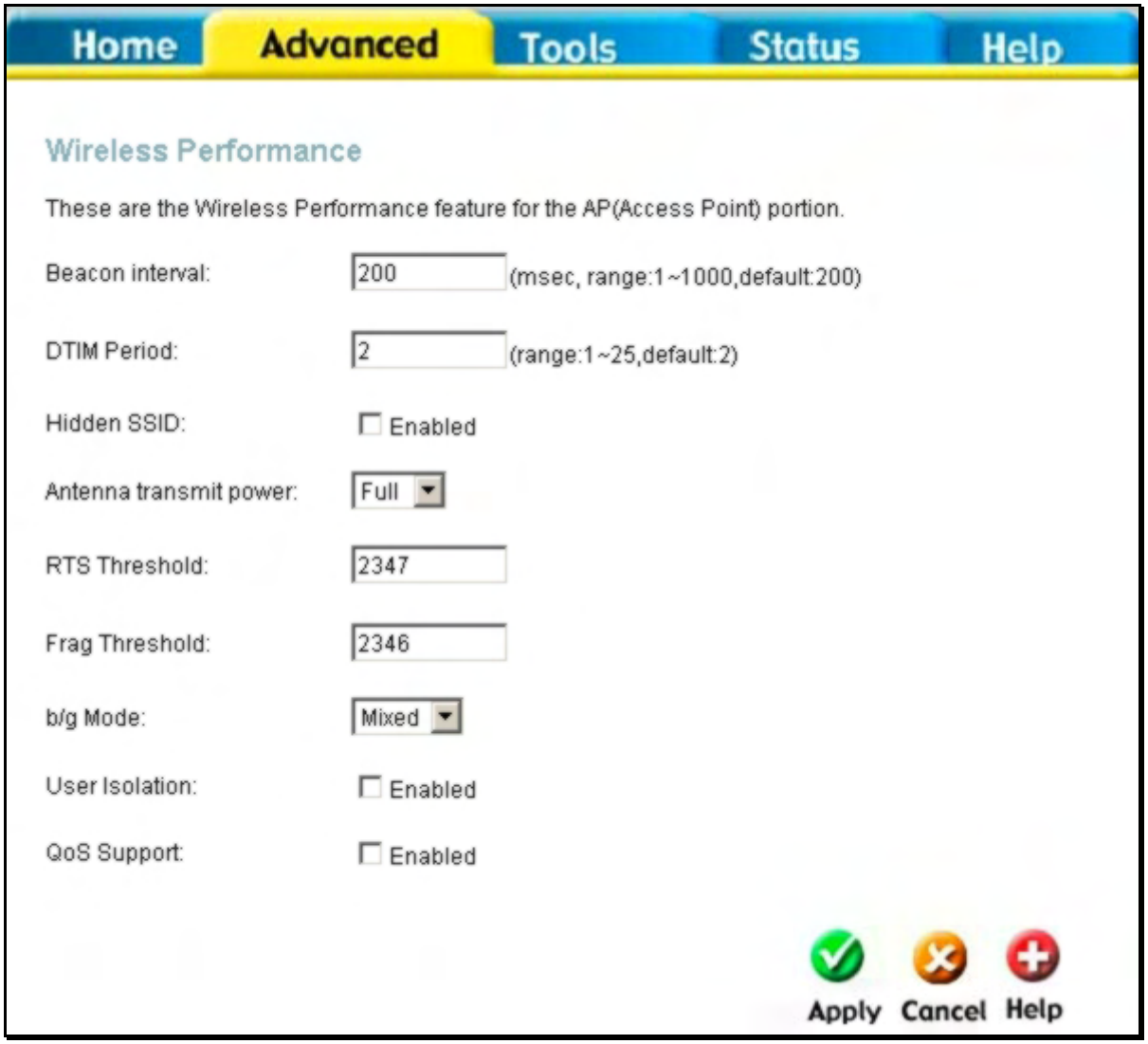
WDS Mode	Parameters
Bridge Mode	In bridge mode, the access point communicates only with other access points. No wireless clients can associate with an access point in bridge mode. In bridge mode, the access point has the option of acting as a **Root** (click the **Activate as Root** box to enable). In Root mode the AP becomes a primary link for the Wireless LAN to the Ethernet and Internet. As the Root access point, there cannot be a wireless Uplink through the AP. Only wireless Downlinks may be designated. To designate a Downlink, enable up to 4 downlinks (Downlink 1 – 4) and type the MAC address of the AP used for downlink in the space provided. Use Bridge mode if you are using the access point to connect to a distant Ethernet LAN.
Repeater Mode	In repeater mode the access point can communicate with other access points and wireless clients. Note that repeater mode will limit the amount of throughput of wireless clients to the Ethernet. As with bridge mode, repeater mode allows the AP to function as the Root.
Crude Mode	Crude Mode is recommended for wireless LANs using multiple vendors wireless chip solutions. If wireless stations are using TI chips, use Bridge or Repeater modes.

Note

Consider using a separate IP domain or VLAN for the Wireless LAN, especially when using WDS. Wireless throughput can be severely affected by broadcasts (ARP requests) from the Ethernet when using WDS.

Wireless Performance

The **Wireless Performance** window is used to configure settings for the Access Point feature of this device. Configuring these settings may increase the performance of your router but if you are not familiar with networking devices and protocols, this section should be left at its default settings. Below is a list of the functions associated with the Access Point feature of the router. Click **Apply** when you have completed your changes.



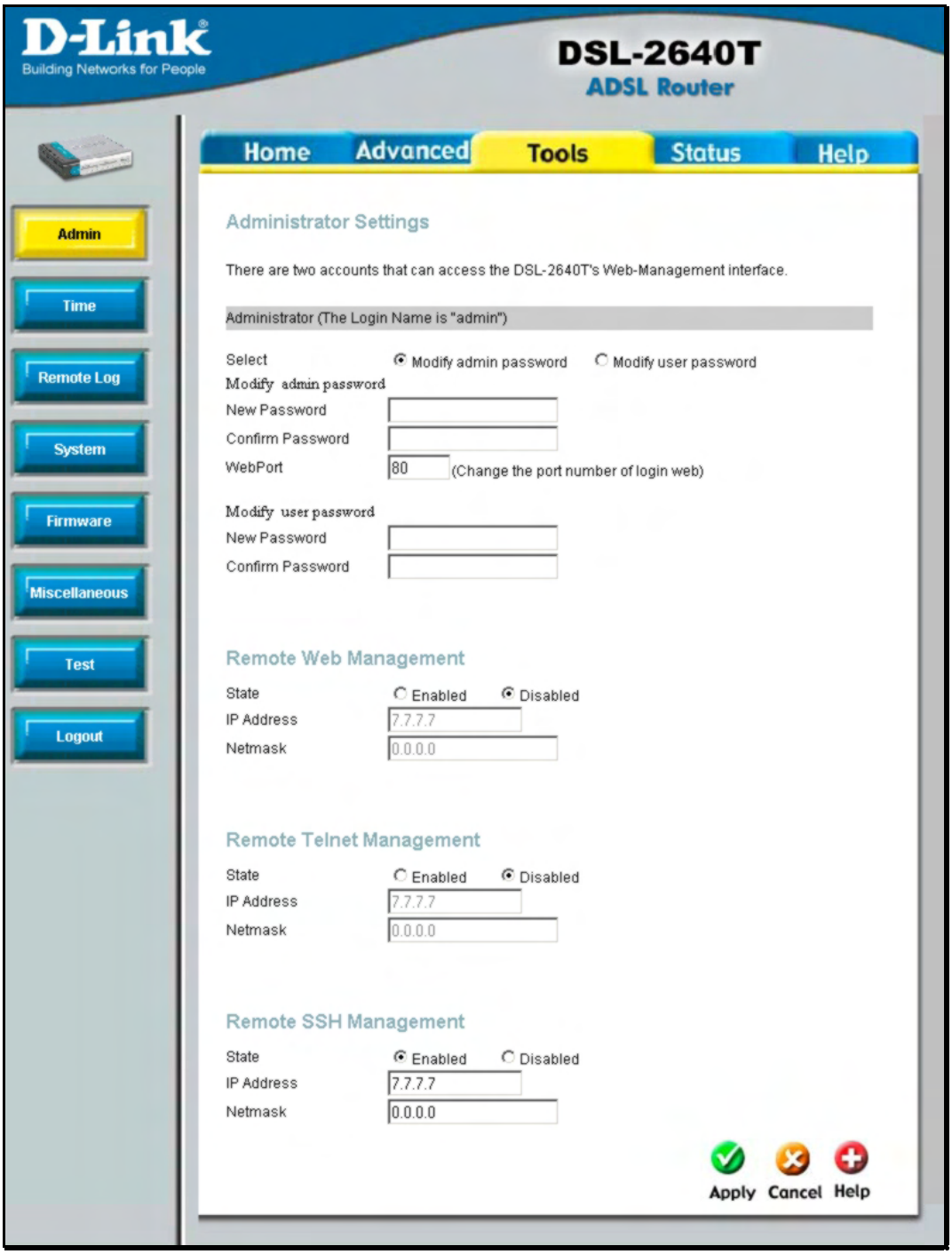
Wireless Performance menu

See the table below for a description of Wireless Performance menu parameters.

Performance Parameter	Description
Beacon Interval	Beacons are emitted from the router in order to synchronize the wireless network. You may set the Beacon Interval range between 20-100 microseconds per beacon sent. The default is 100.
DTIM Period	DTIM (Delivery Traffic Indication Message) Period is a countdown informing clients of the next window for listening to broadcast and multicast messages. The default setting is 3.
Hidden SSID	Choose **Enabled** to STOP broadcasting the SSID across the network. When this is enabled, the SSID willl be hidden from roaming devices. Choose **Disabled** if you want to broadcast the SSID over the network.
Antenna transmit power	Allows the user to adjust the transmit power of the router. A high transmit power allows a greater area range of accessibility to the router. When multiple overlapping access points are present, it may be desirable to reduce transmition power.
RTS Threshold	The RTS (Request to Send) Threshold controls the size of data packets issued to a RTS packet. A lower level will send packets more frequently which may consume a great amount of the available bandwidth. A high threshold will allow the router to recover from interference or collisions which is more prevalent in a network with high traffic or high electromagnetic interference. The default setting is 2347.
Frag Threshold	The fragmentation threshold will determine if packets are to be fragmented. Packets over the 2346 byte limit will be fragmented before transmission. 2346 is the default setting.
b/g Mode	The access point can be forced to operate in g mode or b mode to associate with exclusively 802.11b or 802.11g devices. Additional options include b+ and g+, these are enhanced higher speed operation modes for 802.11b and 802.11g devices that support it.
User Isolation	When User Isolation is enabled, peer-to-peer communication is disabled. This prevents unicasts from one wirless station to another in the same BSS.
QoS Support	Select to enable wireless QoS priority (IEEE 802.11e) support.

Tools

Click the **Tools** tab to reveal the window buttons for various functions located in this directory. The **Administrator Settings** window is the first item in the **Tools** directory. This window is used to change the system password used to access the web manager, to save or load Router configuration settings and to restore default settings. The functions in this and the other **Tools** windows are described below.

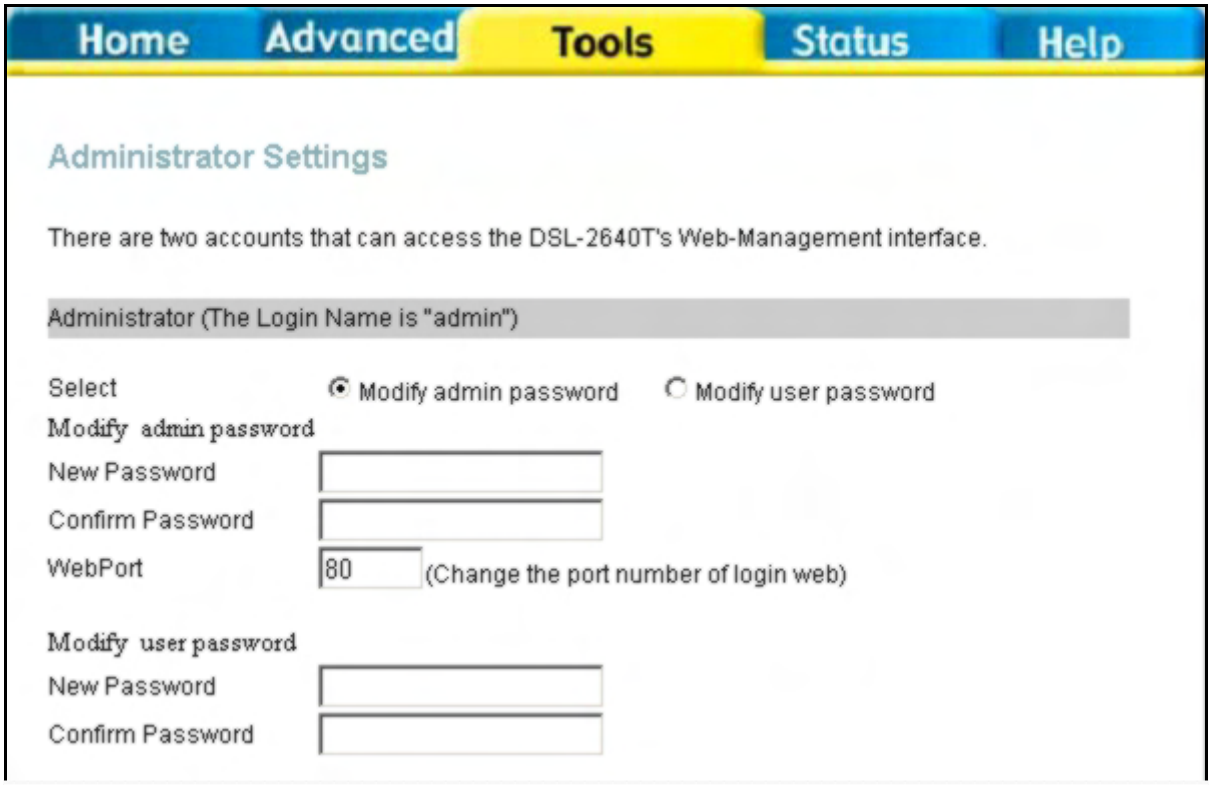


Administrator Settings window

Change System Password

Click the **Admin** button in the **Tools** directory to view the the **Administrator Settings** menu. Select the password level being changed, click the **Modify admin password** option to change Admistrator level password or **Modify user password** option to change the user level password. If you are changing the Administrator's password, type the **New Password** and **Confirm Password** to be certain you have typed it correctly in the **Modify admin password**. If you are changing the User's password, type the **New Password** and **Confirm Password** to be certain you have typed it correctly in the **Modify user password**. Click the **Apply** button to activate the new password. The System User Name remains "admin", this cannot be changed using the web manager interface.

You may also use this menu to change the TCP **WebPort** used to access the web manager. This will not change the port used by computers to access the Internet.



Administrator Settings menu (top portion of Tools>Admin menu)

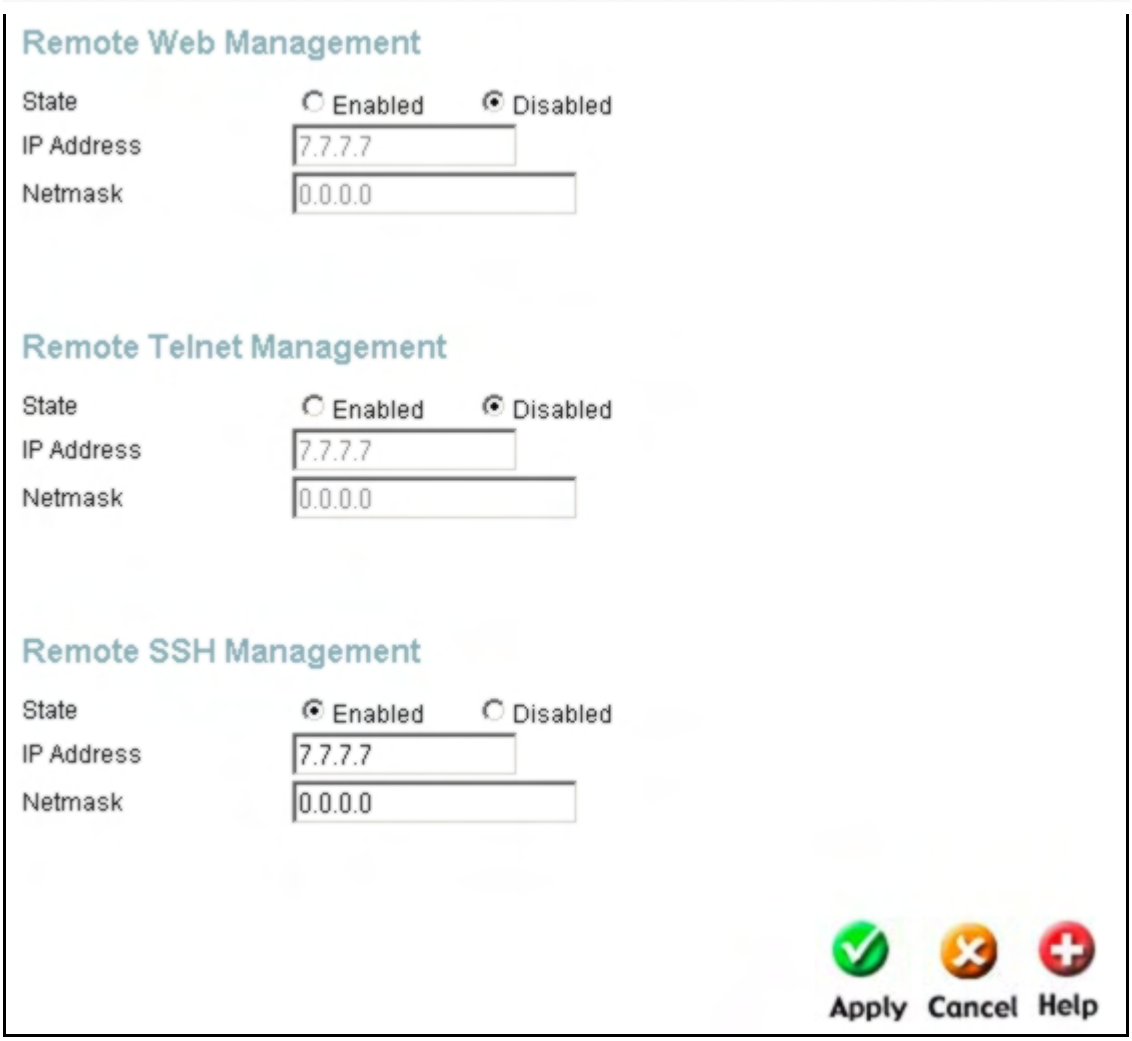
Note

The User level password allows limited access to status displays of the Router.

Remote Web Management and Remote Telnet Access

The **Administrator Settings** window is also used to enable remote Telnet management, remote SSH management and remote web management access to the Router.

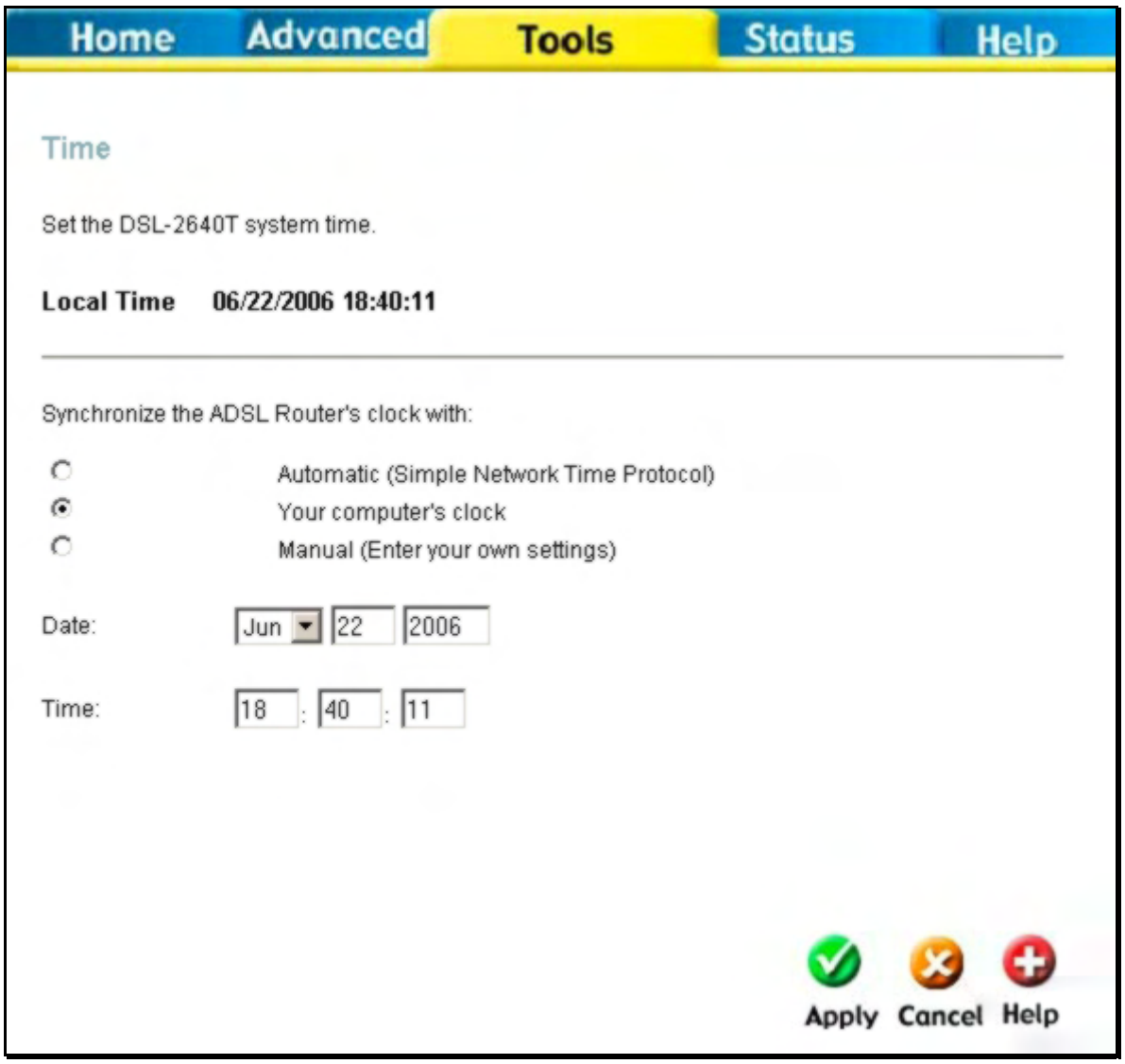
In each case, the procedure to enable remote management of the Router is the same. First, select the **State** Enabled radio button for **Remote Web Management**, **Remote Telnet Management**, or **Remote SSH Management**, and then type the IP Address and Netmask of the remote network or system used for management. Finally, click the **Apply** button to activate remote management from the chosen IP address. Be sure to save the new setting.



Remote Management (lower portion of Tools>Admin menu)

Time

The Router provides a number of options to maintain current date and time including SNTP.



Time menu

To configure system time on the Router, select the method used to maintain time. The options available include SNTP, using your computer's system clock (default) or set the time and date manually. If you opt to use SNTP, you must enter the SNTP server URL or IP address. Click the **Apply** button to set the system time.

Remote Log

Us the **Remote Log Settings** window to set up logging to servers or computers that are located outside the LAN or subnet of the Router.

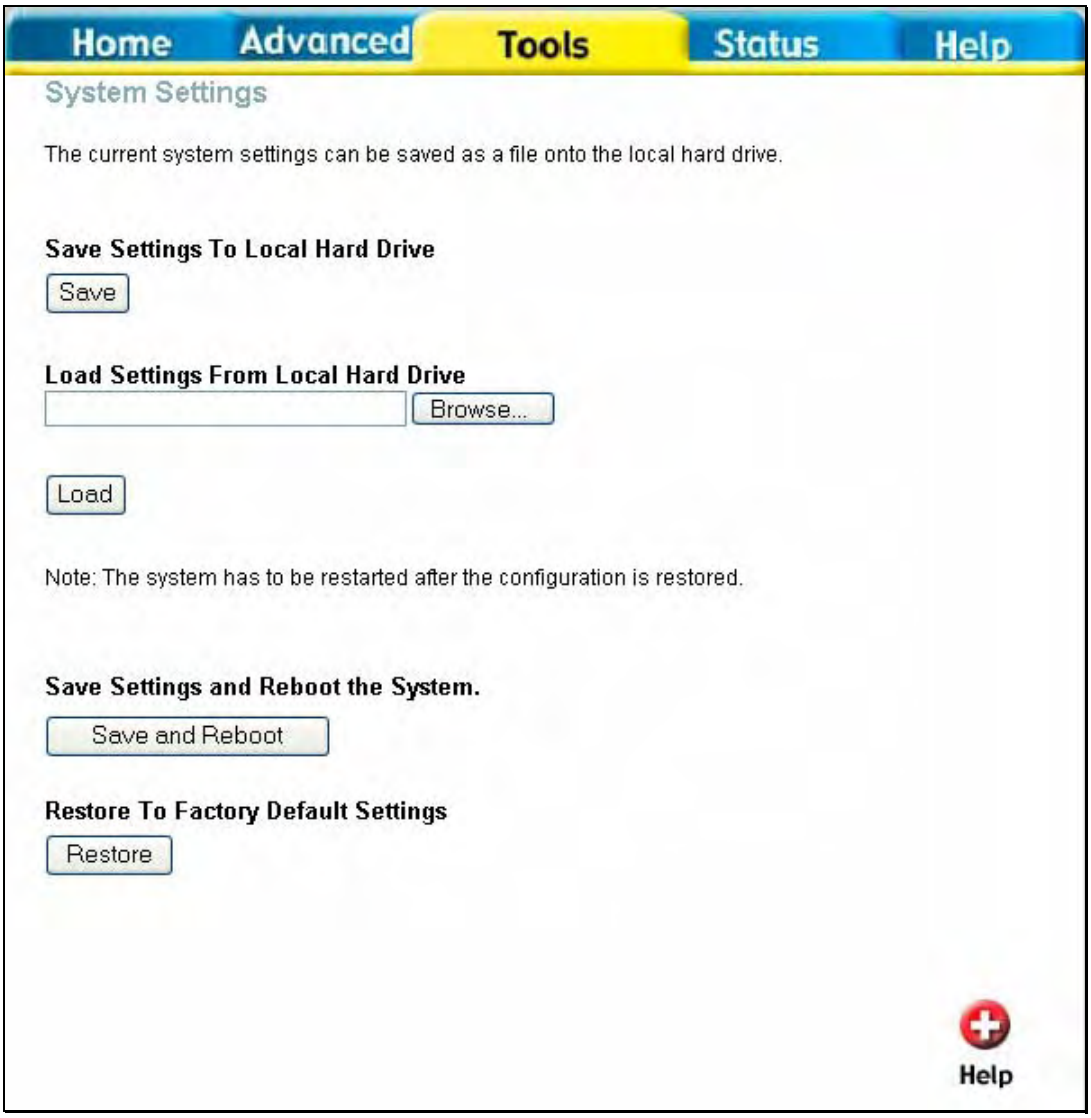
Remote Log Settings window

Select the **Log Level** from the pull-down menu. The levels available are: *Alert, Critical, Debug, Error, Info, Notice, Panic* and *Warning.* Type in the IP address of a receiver for the log message in the **Add an IP Address** field and click on the **Add** button. Log message receivers that are added appear listed in the **Select a logging destination** pull-down menu. These may be used at any time for other types of log messages. To remove a log message receiver from the list, select it and click on the **Remove** button. Click the **Apply** button when you have configured the log message receivers. Remember to save the settings to non-volatile memory.

Save or Load Configuration File

Once you have configured the Router to your satisfaction, it is a good idea to back up the configuration file to your computer. To save the current configuration settings to your computer, click the **System** button in the **Tools** directory to display the **System Settings** window. Click the **Save** button to Save Settings to Local Hard Drive. You will be prompted to select a location on your computer to put the file. The file type is .xml (HTML) and may be named anything you wish.

To load a previously saved configuration file, click the **Browse** button and locate the file on your computer. Click the **Load** button to Load Settings From Local Hard Drive. Confirm that you want to load the file when prompted and the process is completed automatically. The Router will reboot and begin operating with the configuration settings that have just been loaded.



System Settings window

Restore Factory Default Settings

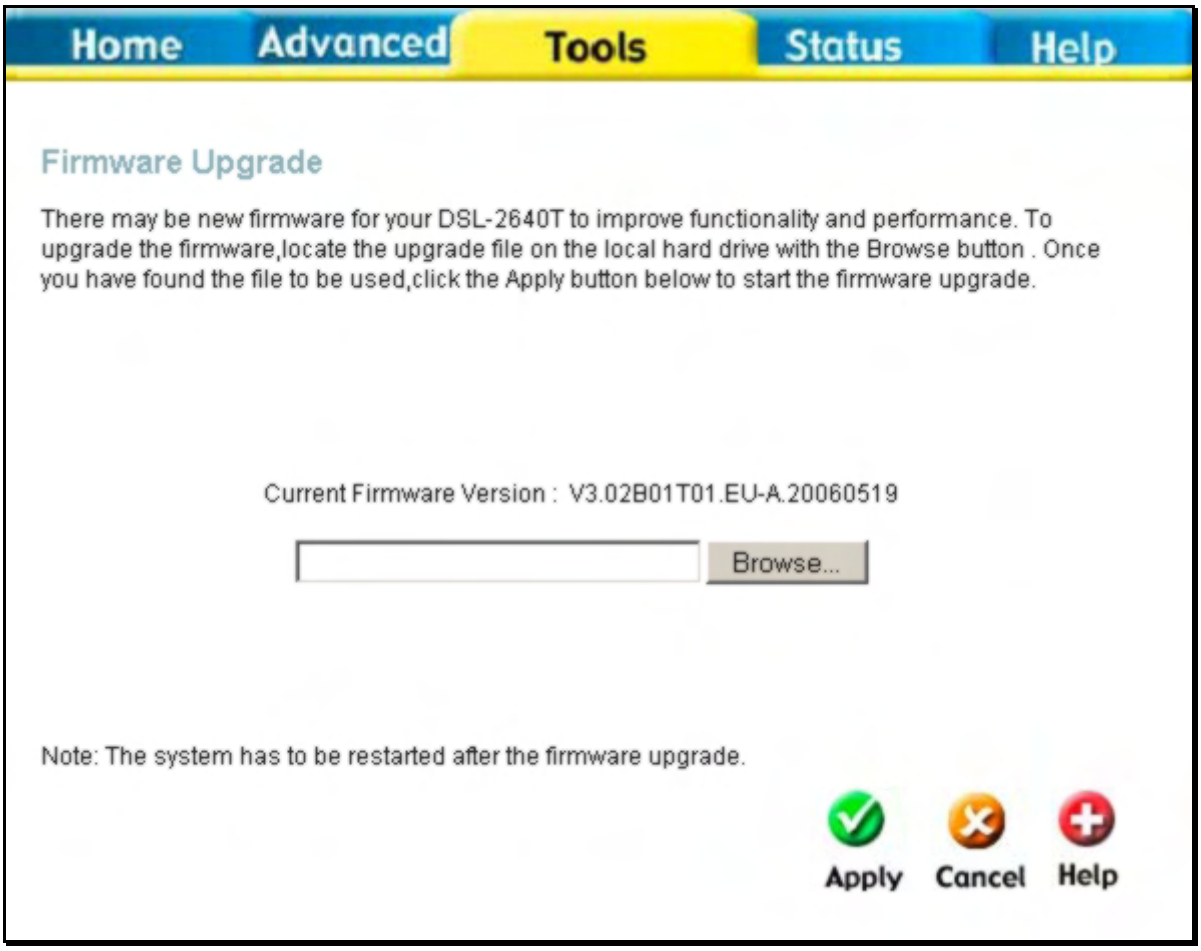
To reset the Router to its factory default settings, click the **Restore** button. You will be prompted to confirm your decision to reset the Router. The Router will reboot with the factory default settings including IP settings (192.168.1.1) and Administrator password (admin).

Firmware Upgrade

Note

Performing a Firmware Upgrade can sometimes change the configuration settings. Be sure to back-up the Router's configuration settings before upgrading the firmware.

Use the **Firmware Upgrade** window to load the latest firmware for the device. Note that the device configuration settings may return to the factory default settings, so make sure you save the configuration settings with the **System Settings** window described above.

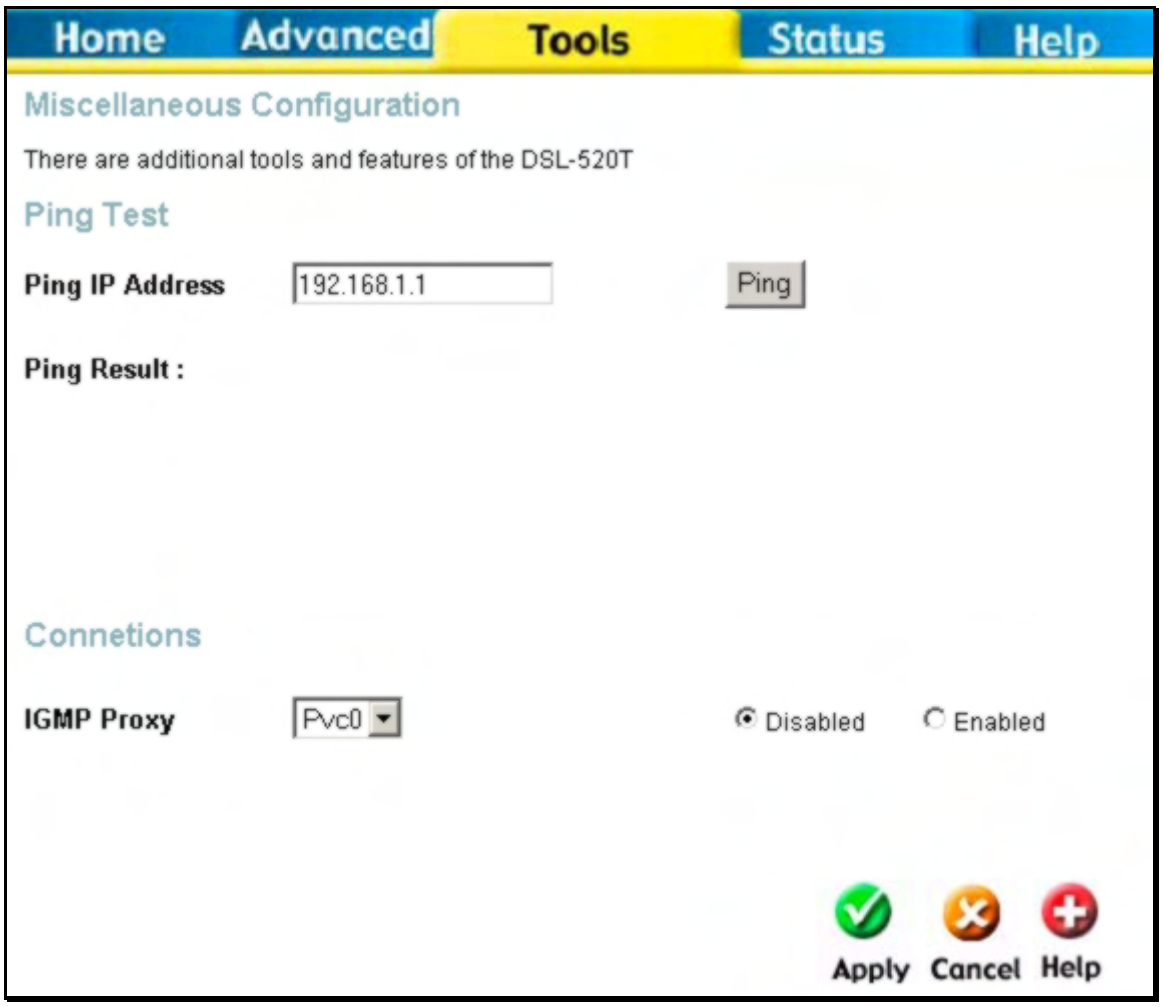

Home
Advanced
Tools
Status
Help
Firmware Upgrade
There may be new firmware for your DSL-2640T to improve functionality and performance. To upgrade the firmware,locate the upgrade file on the local hard drive with the Browse button . Once you have found the file to be used,click the Apply button below to start the firmware upgrade.
Current Firmware Version : V3.02B01T01.EU-A.20060519
Browse...
Note: The system has to be restarted after the firmware upgrade.
Apply
Cancel
Help

Firmware Upgrade menu

To upgrade firmware, type in the name and path of the file or click on the **Browse** button to search for the file. Click the **Apply** button to begin copying the file. The file will load and restart the Router automatically.

Miscellaneous Configuration

To perform a statndard Ping test for network connectivity, click the **Misc.** window button in the **Tools** directory to view the **Miscellaneous Configuration** window.



Miscellaneous Configuration window

Other functions available in Miscellaneous Configuration menu are a Ping test and IGMP enable/disable.

Ping Test

The Ping test functions on the WAN and LAN interfaces. Type the IP address you want to check in the space provided and click the **Ping** button. Read the Ping test result in the space immediately below.

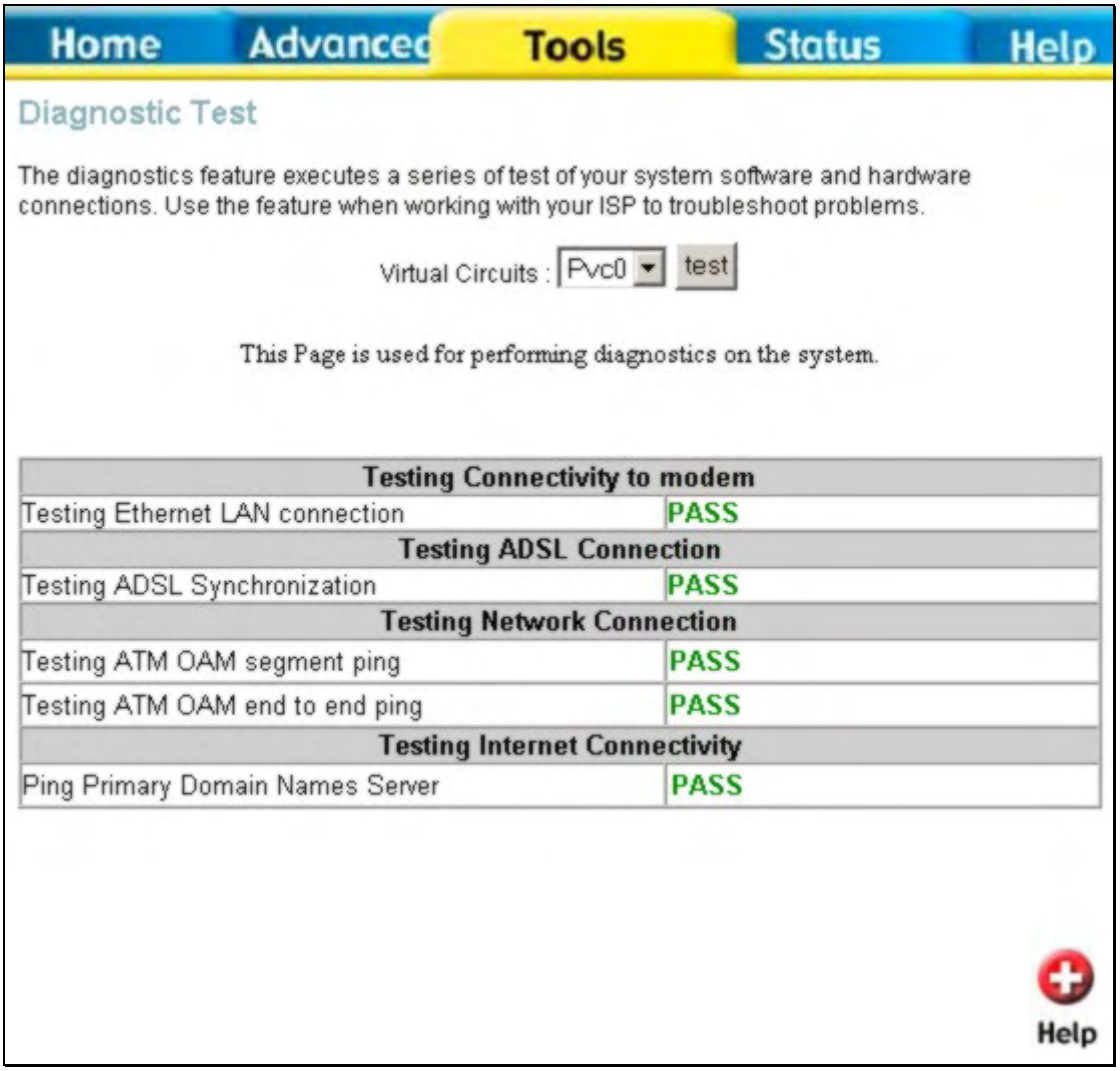
IGMP Proxy

The **Miscellaneous Configuration** window also allows you to enable IGMP forwarding.

This is disabled by default. This setting will not allow IGMP (Internet Group Management Protocol) packets to be forwarded to the LAN. IGMP is used to manage multicasting on TCP/IP networks—most users will not need to enable this. Some ISPs use IGMP to perform remote configuration for client devices, such as the Router. If you are unsure, please check with your ISP. To enable IGMP service to the LAN interface, select **Enabled** and click the **Apply** button.

Diagnostic Test

The **Diagnostic Test** window is used to test connectivity of the Router. A Ping test may be done through the local or external interface to test connectivity to known IP addresses. The diagnostics feature executes a series of test of your system software and hardware connections. Use this window when working with your ISP to troubleshoot problems.



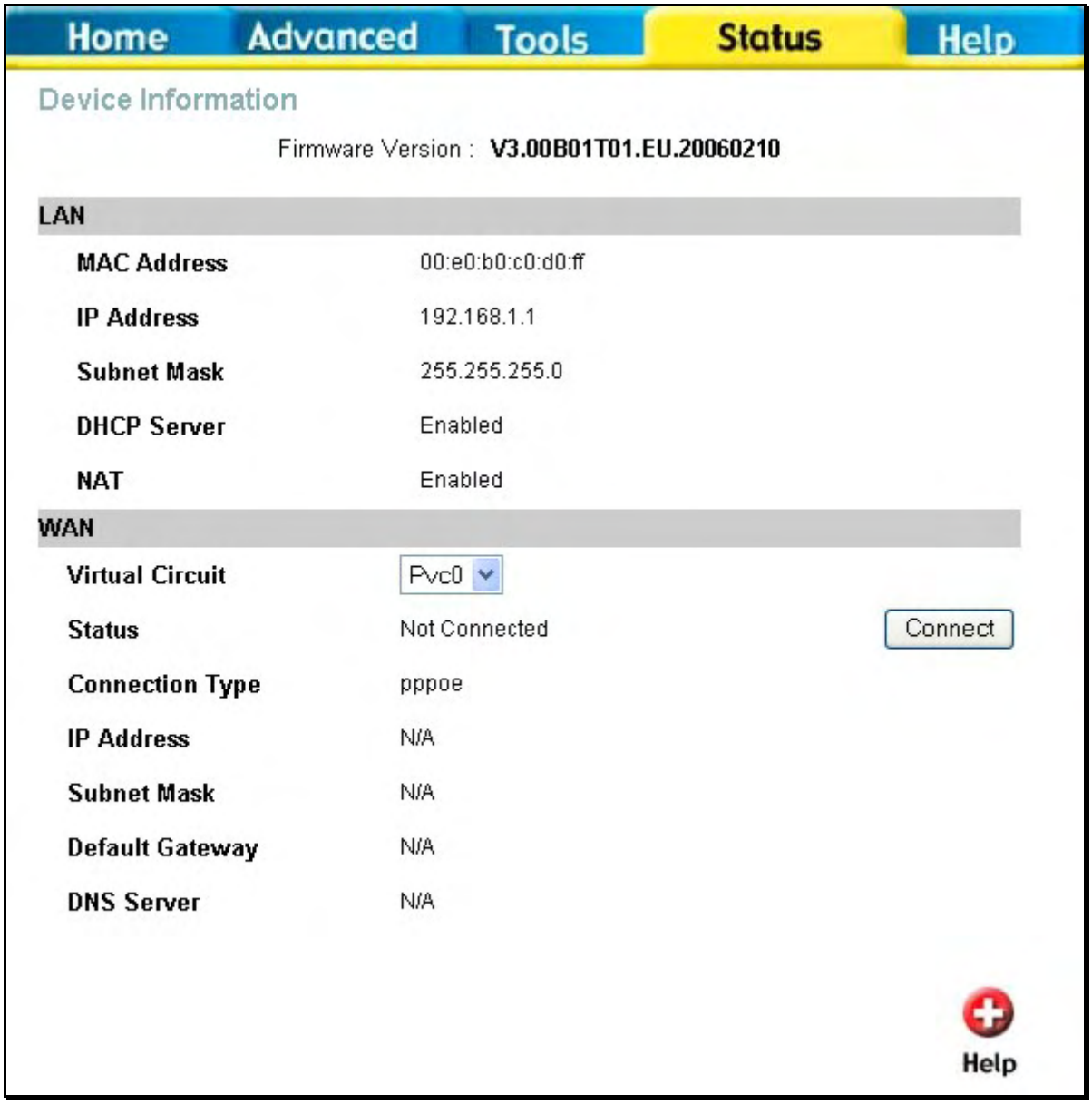
Diagnostic Test window

Status

Use the various read-only windows to view system information and monitor performance.

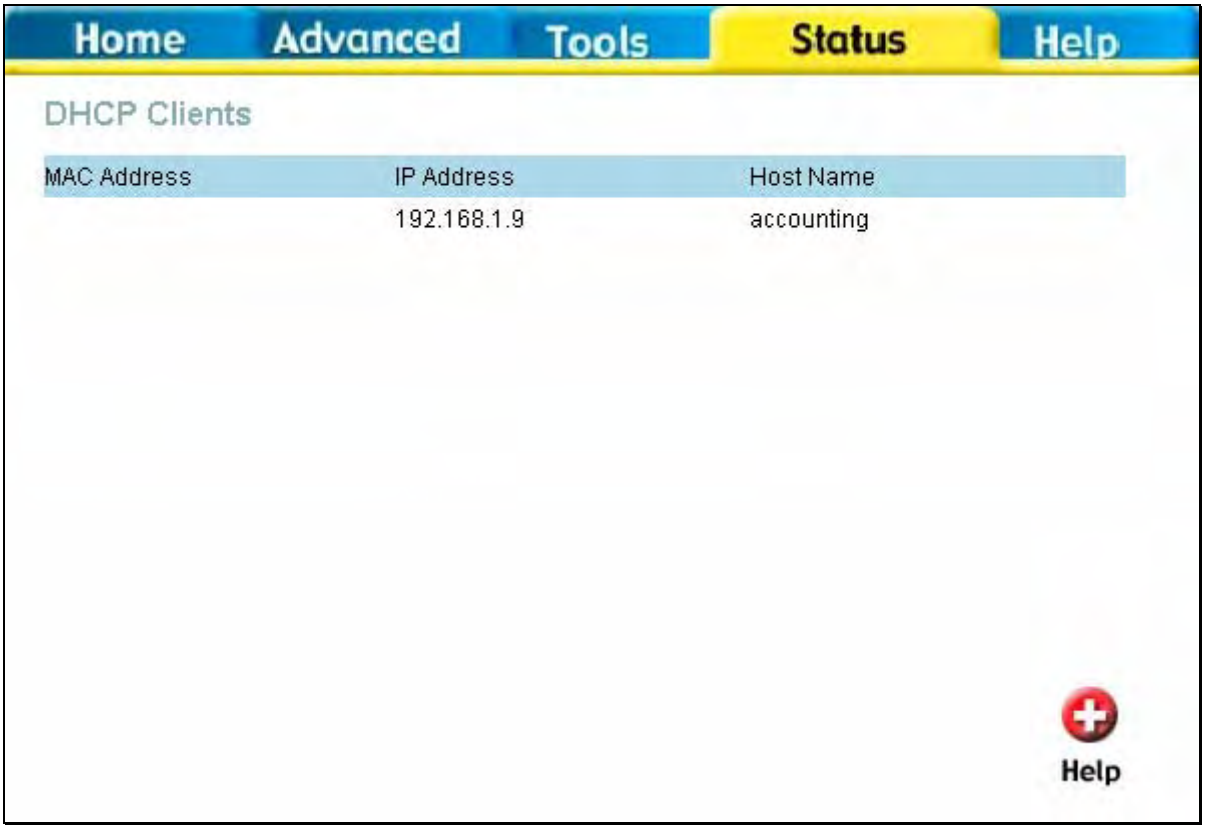
Device Info

Use the **Device Information** window to quickly view basic current information about the LAN and WAN interfaces and device information including Firmware Version and MAC address.



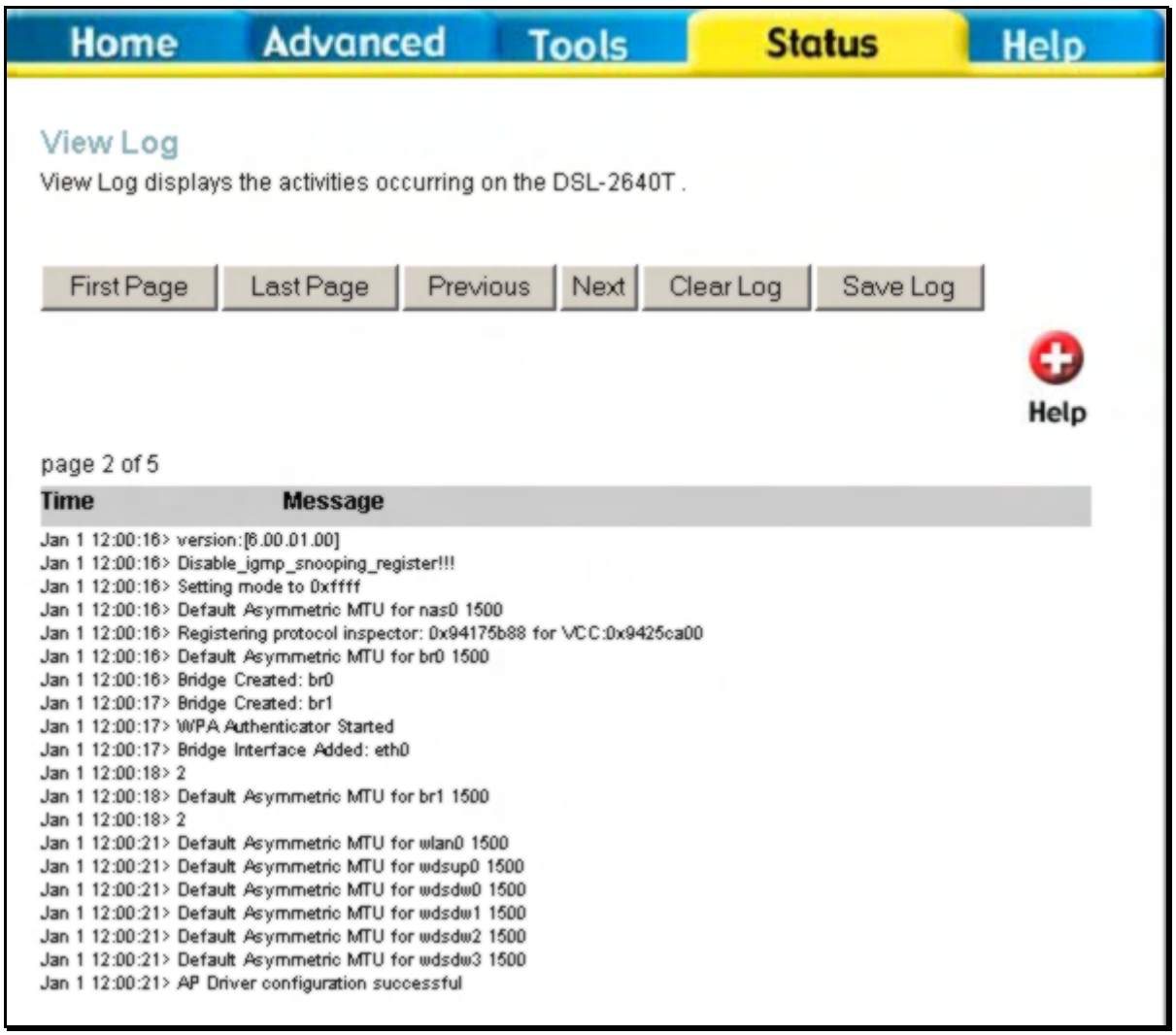
Device Information window

DHCP Clients



Log

The system log displays chronological event log data. Use the navigation buttons to view or scroll log pages. You may also save a simple text file containing the log to your computer. Click the **Save Log** button and follow the prompts to save the file.

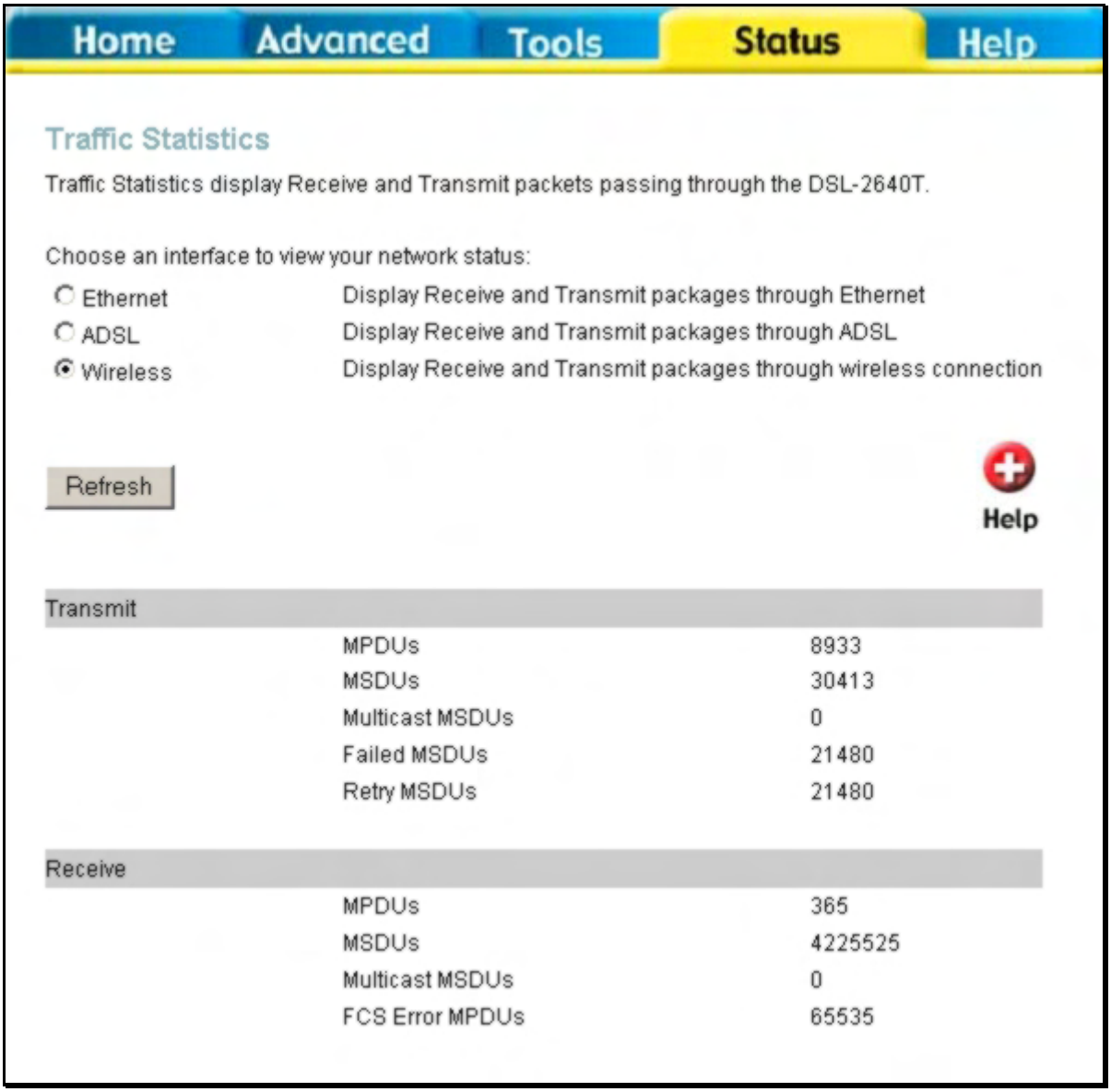

Home
Advanced
Tools
Status
Help
View Log
View Log displays the activities occurring on the DSL-2640T .
First Page
Last Page
Previous
Next
Clear Log
Save Log
Help
page 2 of 5
Time
Message
Jan 1 12:00:16> version:[6.00.01.00]
Jan 1 12:00:16> Disable_igmp_snooping_register!!!
Jan 1 12:00:16> Setting mode to 0xffff
Jan 1 12:00:16> Default Asymmetric MTU for nas0 1500
Jan 1 12:00:16> Registering protocol inspector: 0x94175b88 for VCC:0x9425ca00
Jan 1 12:00:16> Default Asymmetric MTU for br0 1500
Jan 1 12:00:16> Bridge Created: br0
Jan 1 12:00:17> Bridge Created: br1
Jan 1 12:00:17> WPA Authenticator Started
Jan 1 12:00:17> Bridge Interface Added: eth0
Jan 1 12:00:18> 2
Jan 1 12:00:18> Default Asymmetric MTU for br1 1500
Jan 1 12:00:18> 2
Jan 1 12:00:21> Default Asymmetric MTU for wlan0 1500
Jan 1 12:00:21> Default Asymmetric MTU for wdsup0 1500
Jan 1 12:00:21> Default Asymmetric MTU for wdsdw0 1500
Jan 1 12:00:21> Default Asymmetric MTU for wdsdw1 1500
Jan 1 12:00:21> Default Asymmetric MTU for wdsdw2 1500
Jan 1 12:00:21> Default Asymmetric MTU for wdsdw3 1500
Jan 1 12:00:21> AP Driver configuration successful

View Log window

Click **Clear Log** to delete the current log information.

Statistics

Use the **Traffic Statistics** window to monitor traffic on the Ethernet, or ADSL connection. Select the interface for which you want to view packet statistics and the information will appear below.

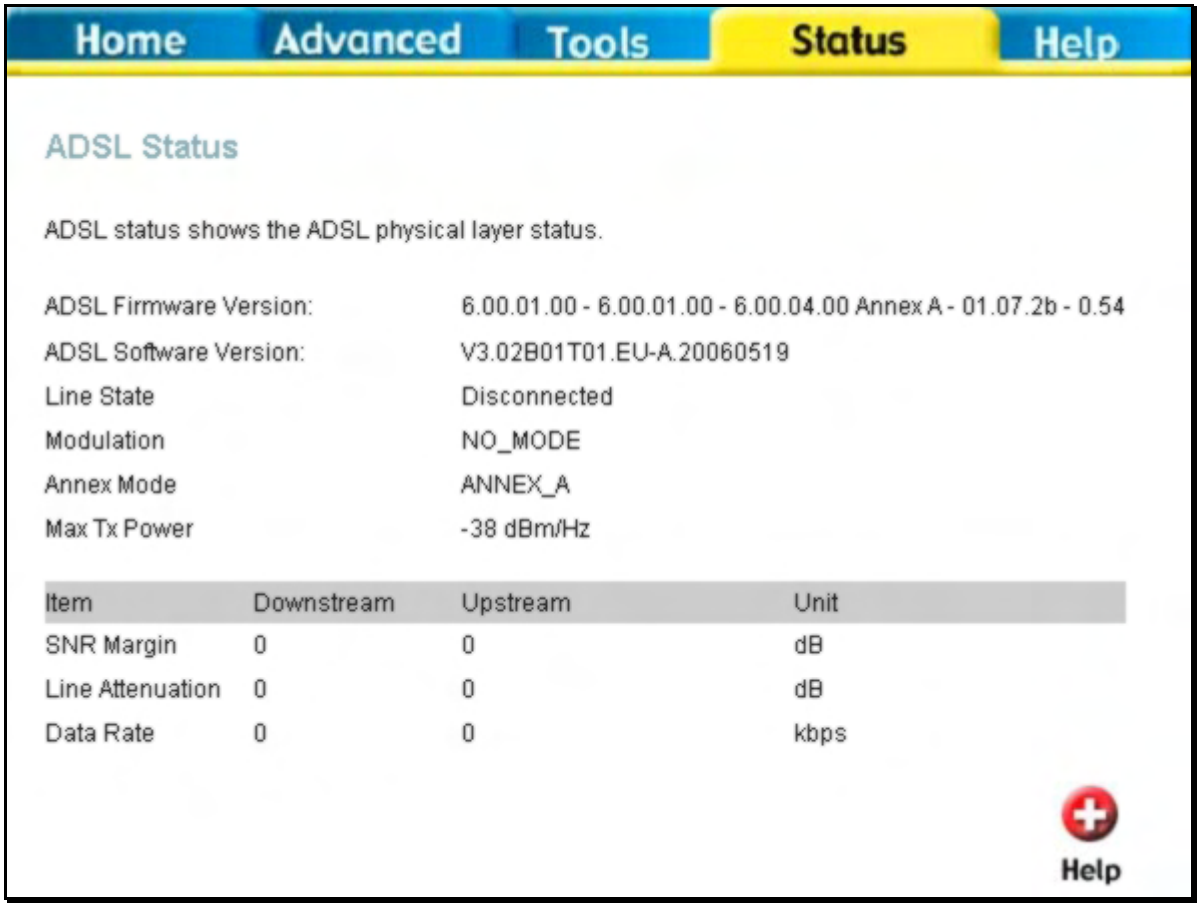


Traffic Statistics window

Click **Refresh** to view traffic information.

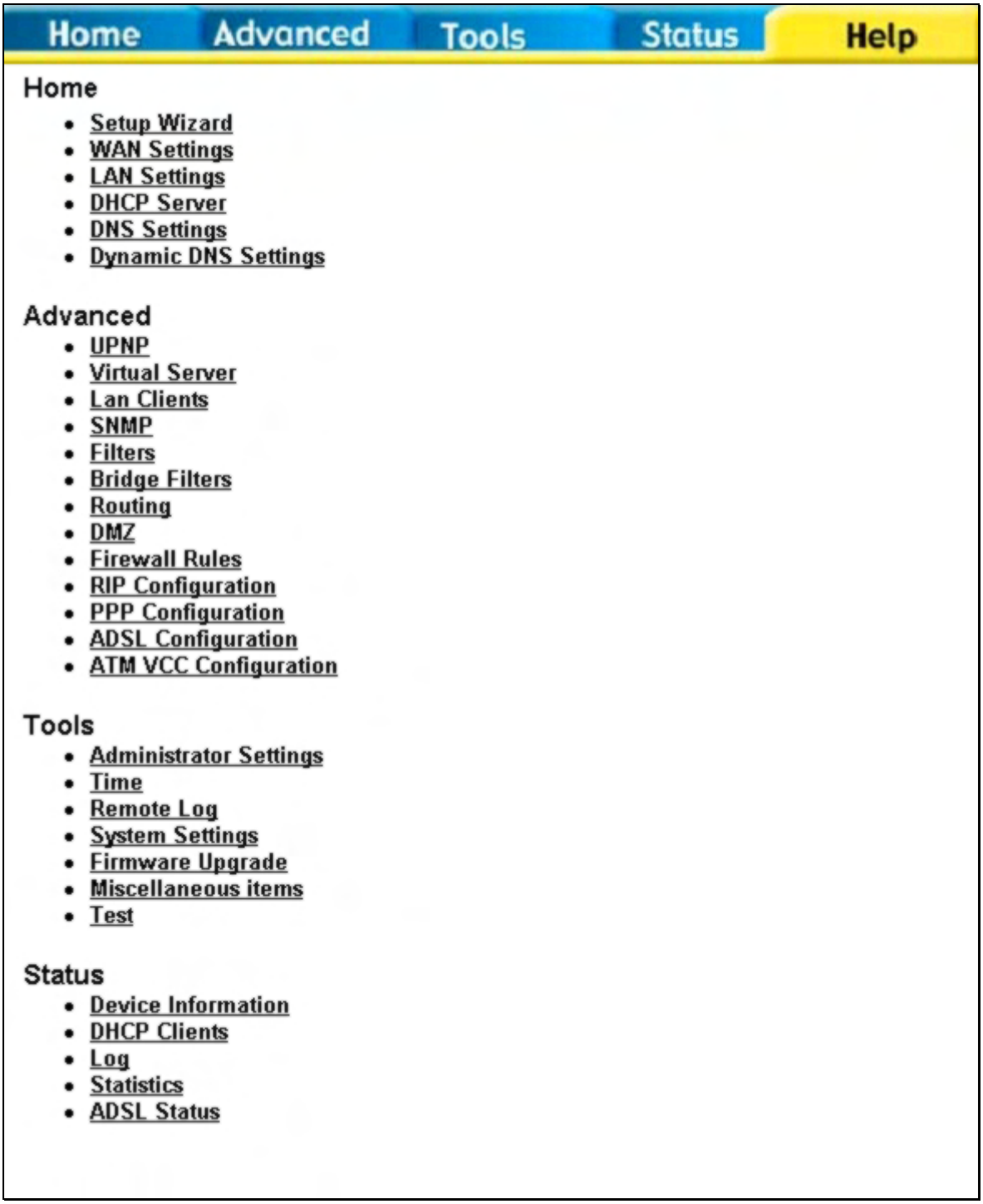
ADSL Status

Use the **ADSL Status** window for troubleshooting the ADSL connection.



ADSL Status information

Help



Help window

Click the desired hyperlink to access help files.

A

Technical Specifications

General		
ADSL Standards:	**ADSL Standards** • ANSI T1.413 Issue 2 • ITU G.992.1 (G.dmt) Annex A • ITU G.992.2 (G.lite) Annex A • ITU G.994.1 (G.hs) • ITU G.992.5 Annex A	**ADSL2 Standards** • ITU G.992.3 (G.dmt.bis) Annex A • ITU G.992.4 (G.lite.bis) Annex A
Protocols:	• IEEE 802.1d Spanning Tree • TCP/UDP • ARP • RARP • ICMP • RFC1058 RIP v1 • RFC1213 SNMP v1 & v2c • RFC1334 PAP • RFC1389 RIP v2	• RFC1483/2684 Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5) • RFC1577 Classical IP over ATM • RFC1661 Point to Point Protocol • RFC1994 CHAP • RFC2131 DHCP Client / DHCP Server • RFC2364 PPP over ATM • RFC2516 PPP over Ethernet
Data Transfer Rate:	• G.dmt full rate downstream: up to 8 Mbps / upstream: up to 1 Mbps • G.lite: ADSL downstream up to 1.5 Mbps / upstream up to 512 Kbps • G.dmt.bis full rate downstream: up to 12 Mbps / upstream: up to 12 Mbps • ADSL full rate downstream: up to 24 Mbps / upstream: up to 1 Mbps	
Media Interface:	• ADSL interface: RJ-11 connector for connection to 24/26 AWG twisted pair telephone line • LAN interface: RJ-45 port for 10/100BASE-T Ethernet connection	

Physical and Environmental	
DC Inputs: **Power Adapter:**	Input: 120V AC 60Hz Output: 12V AC, 1200mA
Power Consumption:	10 Watts (max)
Operating Temperature:	0° to 40°C
Storage Temperature	-20° to 70°C
Humidity:	5% to 95% (non-condensing)
Dimensions:	109 mm x 142.8 mm x 32.1 mm
Weight:	??? gm
EMI:	CE Class B, FCC Class B (Part 15)
Safety:	CSA 950, UL 1950, IEC 60950, EN 60950
Reliability:	Mean Time Between Failure (MTBF) min. 4 years

Wireless	
Standards	IEEE 802.11g, IEEE 802.11b
Modulation	IEEE 802.11b: DQPSK, DBPSK, DSSS, and CCK IEEE 802.11g: BPSK, QPSK, 16QAM, 64QAM, OFDM
Frequency	2.4 GHz to 2.46 GHz (2400 ~ 2484.5MHz ISM band)
Operating Range	Indoors – up to 328 feet (100 meters) Outdoors – up to 1312 feet (400 meters)
Transmit Power	11g: 16dBm Typical 11b: 18dBm Typical
Antenna	Built-in Diversity Antenna (One external Dipole Antenna with RG178 cable assembly) 1) 2.4~2.5Ghz operation mode 2) Peak Gain：2.0 dBi Typical 3) Impedance：50 Ohm nominal 4) V.S.W.R.：2.0:1 Max. 5) Connector：SMA Reverse Connector
Channels	11 channels for United States 13 channels for European Countries 13 channels for Japan
Wireless Data Rates	IEEE 802.11b: 11, 5.5, 2, and 1Mbps IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54Mbps
Media Access Protocol	CSMA/CA with ACK
WEP	64/128/256 bits
Wireless Certification	Wi-Fi WPA

B

Configuring IP Settings on Your Computer

In order to configure your system to receive IP settings from the Router it must first have the TCP/IP protocol installed. If you have an Ethernet port on your computer, it probably already has TCP/IP protocol installed. If you are using Windows XP the TCP/IP is enabled by default for standard installations. Below is an illustrated example of how to configure a Windows XP system to automatically obtain IP settings from the Router. Following this example is a step-by-step description of the procedures used on the other Windows operating systems to first check if the TCP/IP protocol has been installed; if it is not, instructions are provided for installing it. Once the protocol has been installed you can configure the system to receive IP settings from the Router.

For computers running non-Windows operating systems, follow the instructions for your OS that configure the system to receive an IP address from the Router, that is, configure the system to be a DHCP client.

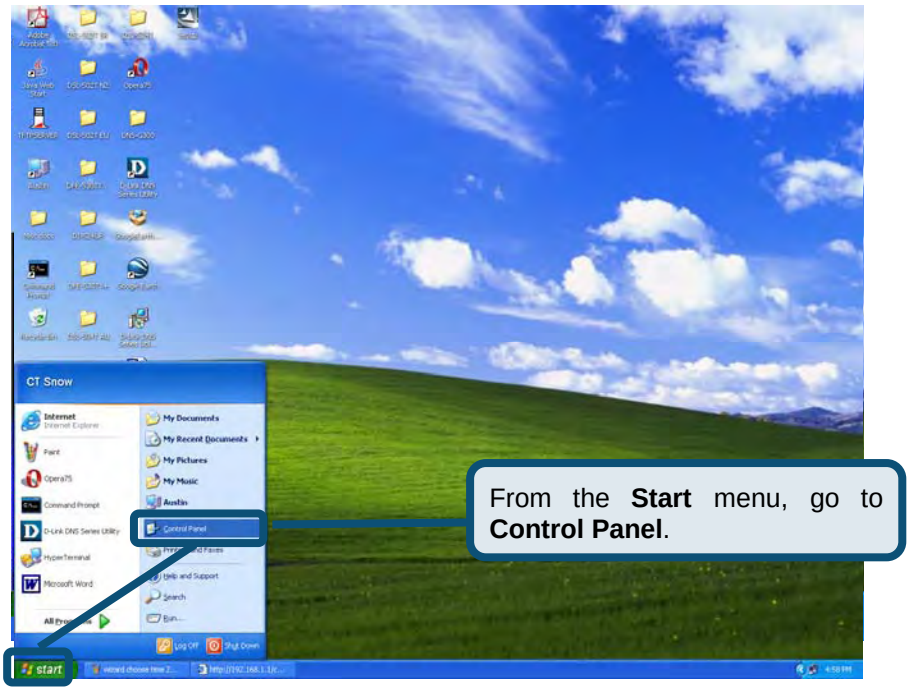
Note

If you are using this Router to provide Internet access for more than one computer, you can use these instructions later to change the IP settings for the other computers. However, you cannot use the same IP address since every computer must have its own IP address that is unique on the local network.

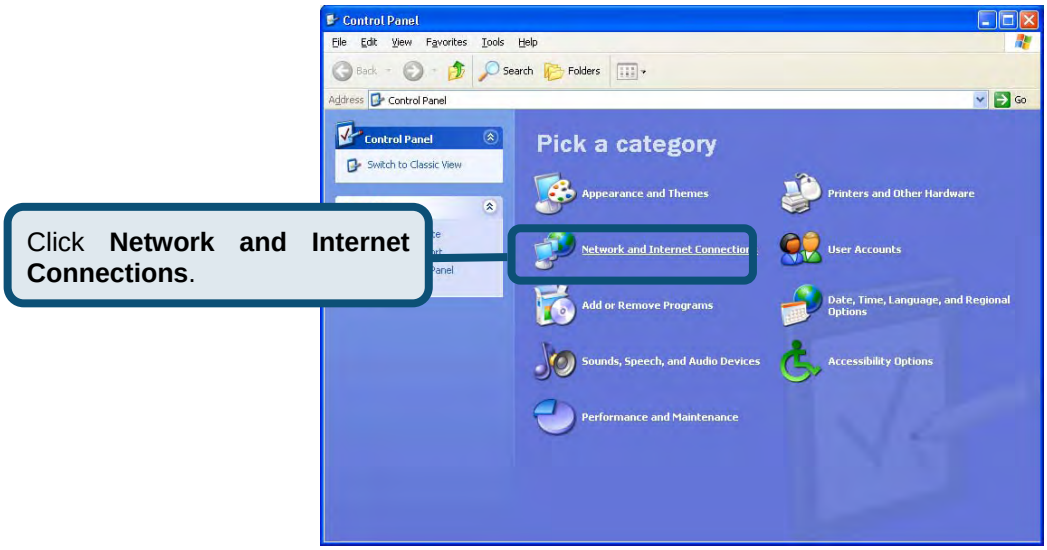
Configure Windows XP for DHCP

Use the following steps to configure a computer running Windows XP to be a DHCP client.

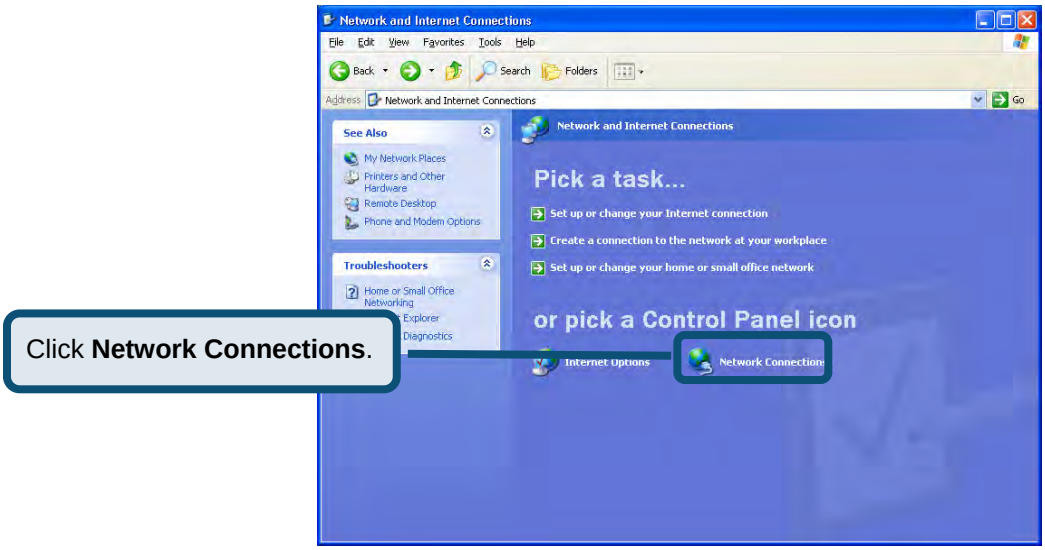
1. From the **Start** menu on your desktop, go to **Control Panel.**



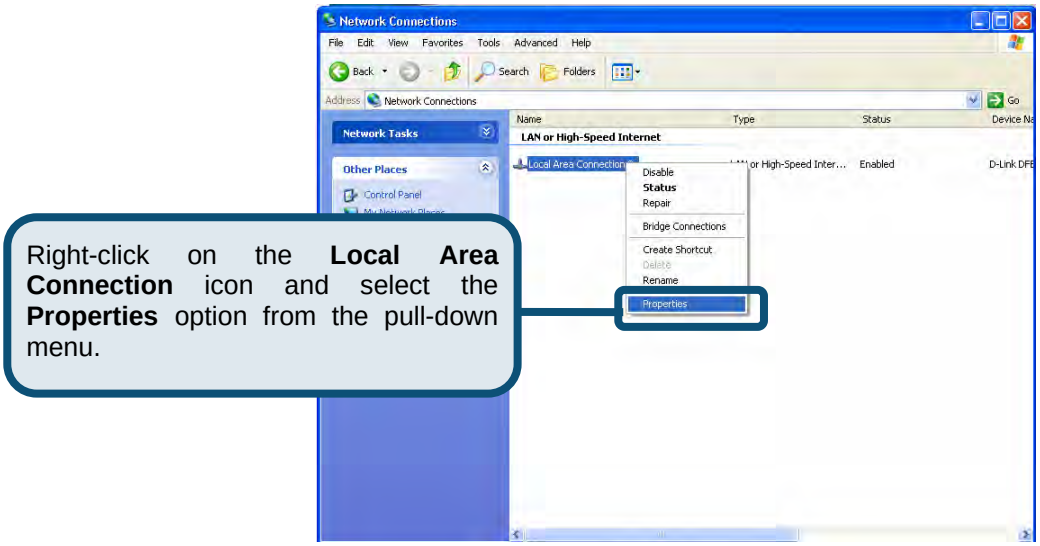
2. In the Control Panel window, click Network and Internet Connections.



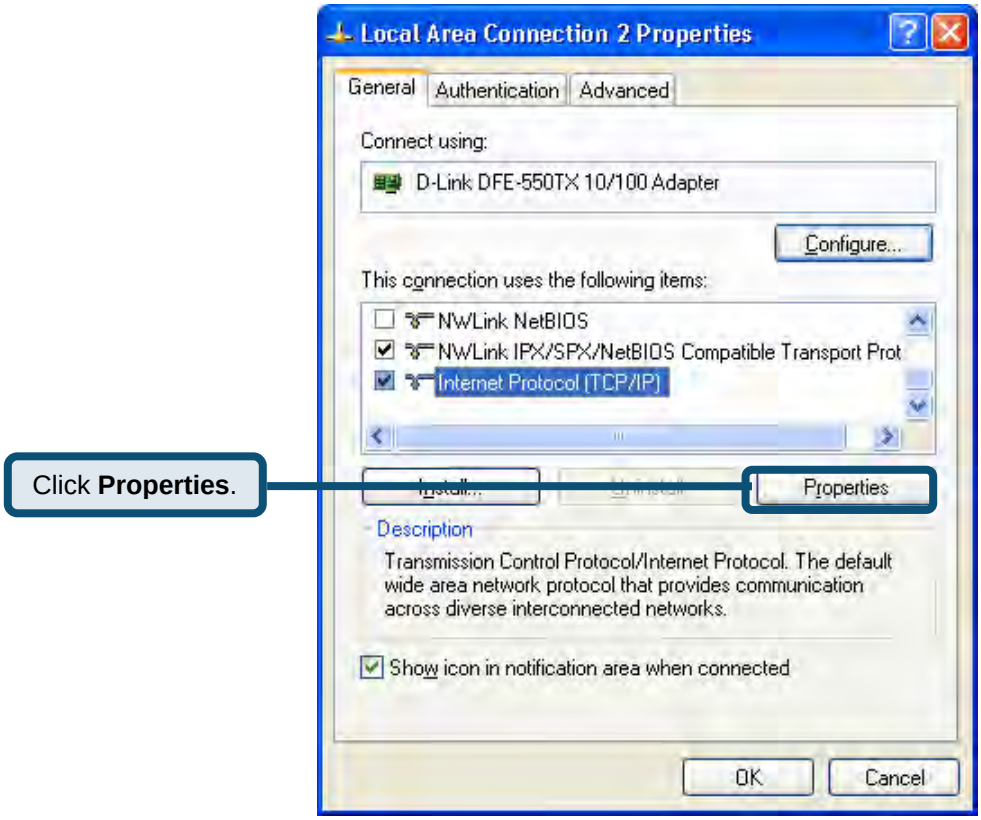
3. In the Network and Internet Connections window, click **Network Connections**.


Network and Internet Connections
File Edit View Favorites Tools Help
Back Search Folders
Address Network and Internet Connections
Go
See Also
My Network Places
Printers and Other Hardware
Remote Desktop
Phone and Modem Options
Troubleshooters
Home or Small Office Networking
Network and Internet Connections
Pick a task...
Set up or change your Internet connection
Create a connection to the network at your workplace
Set up or change your home or small office network
or pick a Control Panel icon
Internet Options
Network Connections
Click Network Connections.

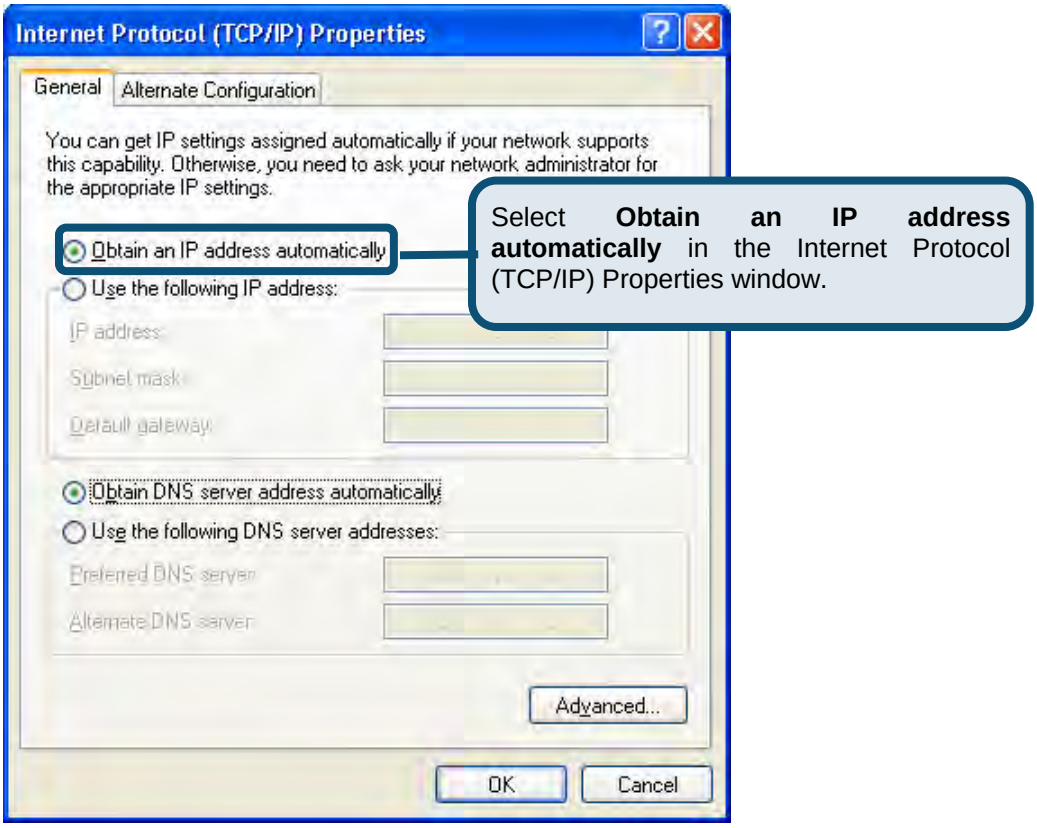
4. In the Network Connections window, right-click on **Local Area Connection**, then click **Properties**.



5. In the **General** tab of the **Local Area Connection Properties** window, highlight **Internet Protocol (TCP/IP)** under "This connection uses the following items:" by clicking on it once. Click on the **Properties** button.



6. Select "Obtain an IP address automatically" by clicking once in the circle. Click the **OK** button


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel
Select **Obtain an IP address automatically** in the Internet Protocol (TCP/IP) Properties window.

Your computer is now ready to use the Router's DHCP server.

Windows 2000

First, check for the IP protocol and, if necessary, install it:

1. In the **Windows** task bar, click the **Start** button, point to **Settings**, and then click **Control Panel**.
2. Double-click the **Network and Dial-up Connections** icon.
3. In the **Network and Dial-up Connections** window, right-click the **Local Area Connection** icon, and then select **Properties**.
4. The **Local Area Connection Properties** dialog box displays with a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled, skip ahead to *Configure Windows 2000 for DHCP*.
5. If Internet Protocol (TCP/IP) does not display as an installed component, click **Install**.
6. In the **Select Network Component Type** dialog box, select **Protocol**, and then click **Add**.
7. Select **Internet Protocol (TCP/IP)** in the Network Protocols list, and then click **OK**.
8. You may be prompted to install files from your Windows 2000 installation CD or other media. Follow the instructions to install the files.
9. If prompted, click **OK** to restart your computer with the new settings.

Configure Windows 2000 for DHCP

1. In the Control Panel, double-click the **Network and Dial-up Connections** icon.
2. In **Network and Dial-up Connections** window, right-click the **Local Area Connection** icon, and then select **Properties**.
3. In the **Local Area Connection Properties** dialog box, select **Internet Protocol (TCP/IP)**, and then click **Properties**.
4. In the **Internet Protocol (TCP/IP) Properties** dialog box, click the button labeled **Obtain an IP address automatically**.
5. Double-click **OK** to confirm and save your changes, and then close the Control Panel.

Your computer is now ready to use the Router's DHCP server.

Windows 95 and Windows 98

First, check for the IP protocol and, if necessary, install it:

1. In the **Windows** task bar, click the **Start** button, point to **Settings**, and then click **Control Panel**. Double-click the **Network** icon.
2. The **Network** dialog box displays with a list of currently installed network components. If the list includes TCP/IP, and then the protocol has already been enabled, skip to *Configure IP Information Windows 95, 98*.
3. If TCP/IP does not display as an installed component, click **Add**. The **Select Network Component Type** dialog box displays.
4. Select **Protocol**, and then click **Add**. The **Select Network Protocol** dialog box displays.
5. Click on **Microsoft** in the Manufacturers list box, and then click **TCP/IP** in the Network Protocols list box.
6. Click **OK** to return to the Network dialog box, and then click **OK** again. You may be prompted to install files from your Windows 95/98 installation CD. Follow the instructions to install the files.
7. Click **OK** to restart the PC and complete the TCP/IP installation.

Configure Windows 95 and Windows 98 for DHCP

1. Open the **Control Panel** window, and then click the **Network** icon.
2. Select the network component labeled TCP/IP, and then click **Properties**.
3. If you have multiple TCP/IP listings, select the listing associated with your network card or adapter.
4. In the **TCP/IP Properties** dialog box, click the **IP Address** tab.
5. Click the **Obtain an IP address automatically** option.
6. Double-click **OK** to confirm and save your changes. You will be prompted to restart Windows.
7. Click **Yes**.

When it has restarted, your computer is ready to use the Router's DHCP server.

Windows ME

First, check for the IP protocol and, if necessary, install it:

1. In the **Windows** task bar, click the **Star**t button, point to **Settings**, and then click **Control Panel**.
2. Double-click the **Network and Dial-up Connections** icon.
3. In the **Network and Dial-up Connections** window, right-click the **Network** icon, and then select **Properties**.
4. The **Network Properties** dialog box displays with a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled. Skip ahead to *Configure Windows ME for DHCP*.
5. If Internet Protocol (TCP/IP) does not display as an installed component, click **Add**.
6. In the **Select Network Component Type** dialog box, select **Protocol**, and then click **Add**.
7. Select **Microsoft** in the Manufacturers box.
8. Select **Internet Protocol (TCP/IP)** in the Network Protocols list, and then click **OK**.
9. You may be prompted to install files from your Windows Me installation CD or other media. Follow the instructions to install the files.
10. If prompted, click **OK** to restart your computer with the new settings.

Configure Windows ME for DHCP

1. In the **Control Panel** window, double-click the **Network and Dial-up Connections** icon.
2. In the **Network and Dial-up Connections** window, right-click the **Network** icon, and then select **Properties**.
3. In the **Network Properties** dialog box, select **TCP/IP**, and then click **Properties**.
4. In the **TCP/IP Settings** dialog box, click the **Obtain and IP address automatically** option.
5. Double-click **OK** twice to confirm and save your changes, and then close the Control Panel.

Your computer is now ready to use the Router's DHCP server.

Windows NT 4.0 Workstations

First, check for the IP protocol and, if necessary, install it:

1. In the **Windows NT** task bar, click the **Start** button, point to **Settings**, and then click **Control Panel**.
2. In the **Control Panel** window, double-click the **Network** icon.
3. In the **Network** dialog box, click the **Protocols** tab.
4. The **Protocols** tab displays a list of currently installed network protocols. If the list includes TCP/IP, then the protocol has already been enabled. Skip to "Configure IP Information"
5. If TCP/IP does not display as an installed component, click **Add**.
6. In the **Select Network Protocol** dialog box, select **TCP/IP**, and then click **OK**. You may be prompted to install files from your Windows NT installation CD or other media. Follow the instructions to install the files.
7. After all files are installed, a window displays to inform you that a TCP/IP service called DHCP can be set up to dynamically assign IP information.
8. Click **Yes** to continue, and then click **OK** if prompted to restart your computer.

Configure Windows NT 4.0 for DHCP

1. Open the **Control Panel** window, and then double-click the **Network** icon.
2. In the **Network** dialog box, click the **Protocols** tab.
3. In the **Protocols** tab, select **TCP/IP**, and then click **Properties**.
4. In the **Microsoft TCP/IP Properties** dialog box, click the **Obtain an IP address automatically** option.
5. Click **OK** twice to confirm and save your changes, and then close the Control Panel.

Your computer is now ready to use the Router's DHCP server.

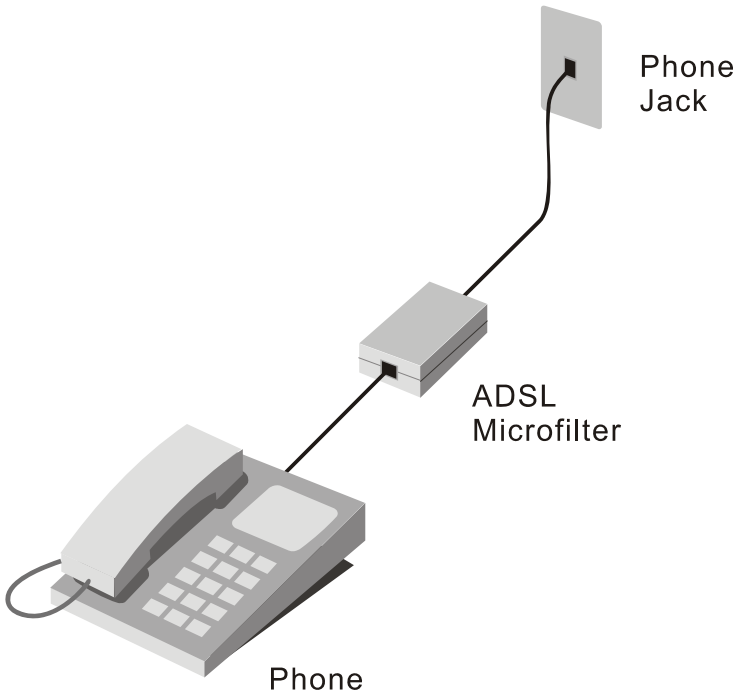
C

Low Pass Filters for DSL

Most ADSL clients will be required to install a simple device that prevents the ADSL line from interfering with regular telephone services. These devices are commonly referred to as microfilters or low pass filters. The two basic styles of low pass filters commonly used are described below.

In-Line Filter

In line low pass filters are used for each telephone or telephone device (answering machines, Faxes etc.) that shares the line with the ADSL service. These devices are attached to the telephone cable between the telephone and wall jack. Filters that install behind the wall plate hidden from view are also available. A typical in-line filter installation is shown in the diagram below.



In-line low pass filter

Three Port Filter

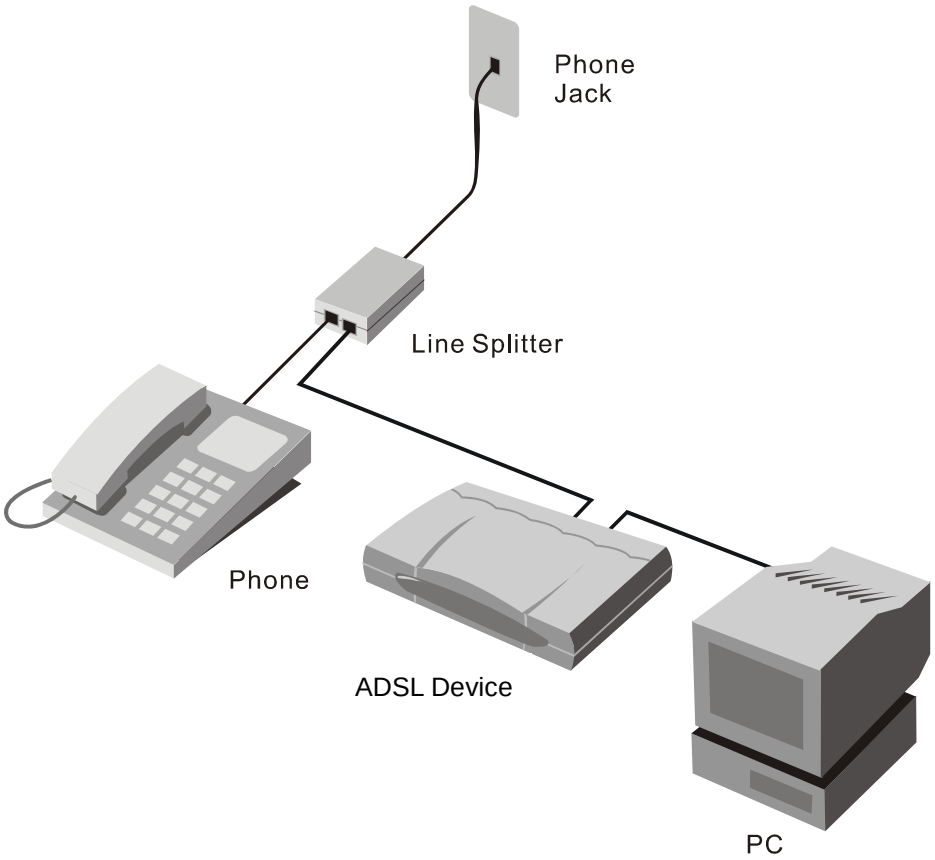
Another style of filter is installed at the same point where the Router connects to the telephone line. Only a single filter is required. The connection ports are typically labeled as follows:

Line - This port connects to the wall jack.

ADSL – This port connects to the Router.

Phone – This port connects to a telephone or other telephone device.

The diagram below illustrates the proper use of this style of filter. Make certain the lines are properly connected. If you are unable to hear a dial tone with the telephone, check the connections to make sure they are securely attached and connected to the correct port.



3-port Filter

D-Link International Offices

U.S.A
17595 Mt. Herrmann Street
Fountain Valley, CA 92708
TEL: 1-800-326-1688
URL: www.dlink.com

Canada
2180 Winston Park Drive
Oakville, Ontario, L6H 5W1
Canada
TEL: 1-905-8295033
FAX: 1-905-8295223
URL: www.dlink.ca

Europe (U. K.)
4th Floor, Merit House
Edgware Road, Colindale
London NW9 5AB
U.K.
TEL: +44-20-8955-9000
FAX: +44-20-8955-9001
URL: www.dlink.co.uk

Germany
Schwalbacher Strasse 74
D-65760 Eschborn
Germany
TEL: 49-6196-77990
FAX: 49-6196-7799300
URL: www.dlink.de

France
No.2 all'ee de la Fresnerie
78330 Fontenay le Fleury
France
TEL: 33-1-30238688
FAX: 33-1-30238689
URL: www.dlink.fr

Netherlands
Weena 290
3012 NJ, Rotterdam
Netherlands
Tel: +31-10-282-1445
Fax: +31-10-282-1331
URL: www.dlink.nl

Belgium
Rue des Colonies 11
B-1000 Brussels
Belgium
Tel: +32(0)2 517 7111
Fax: +32(0)2 517 6500
URL: www.dlink.be

Italy
Via Nino Bonnet n. 6/b
20154 – Milano
Italy
TEL: 39-02-2900-0676
FAX: 39-02-2900-1723
URL: www.dlink.it

Sweden
P.O. Box 15036, S-167 15 Bromma
Sweden
TEL: 46-(0)8564-61900
FAX: 46-(0)8564-61901
URL: www.dlink.se

Denmark
Naverland 2, DK-2600
Glostrup, Copenhagen
Denmark
TEL: 45-43-969040
FAX: 45-43-424347
URL: www.dlink.dk

Norway
Karihaugveien 89
N-1086 Oslo
Norway
TEL: +47 99 300 100
FAX: +47 22 30 95 80
URL: www.dlink.no

Finland
Latokartanontie 7A
FIN-00700 HELSINKI
Finland
TEL: +358-10 309 8840
FAX: +358-10 309 8841
URL: www.dlink.fi

Spain
Avenida Diagonal, 593-95, 9th floor
08014 Barcelona
Spain
TEL: 34 93 4090770
FAX: 34 93 4910795
URL: www.dlink.es

Portugal
Rua Fernando Pahla
50 Edificio Simol
1900 Lisbon Portugal
TEL: +351 21 8688493
URL: www.dlink.es

Czech Republic
Vaclavske namesti 36, Praha 1
Czech Republic
TEL :+420 (603) 276 589
URL: www.dlink.cz

Switzerland
Glatt Tower, 2.OG CH-8301
Glattzentrum Postfach 2.OG
Switzerland
TEL : +41 (0) 1 832 11 00
FAX: +41 (0) 1 832 11 01
URL: www.dlink.ch

Greece
101, Panagoulis Str. 163-43
Helioupolis Athens, Greece
TEL : +30 210 9914 512
FAX: +30 210 9916902
URL: www.dlink.gr

Luxemburg
Rue des Colonies 11,
B-1000 Brussels,
Belgium
TEL: +32 (0)2 517 7111
FAX: +32 (0)2 517 6500
URL: www.dlink.be

Poland
Budynek Aurum ul. Walic-w 11
PL-00-851
Warszawa
Poland
TEL : +48 (0) 22 583 92 75
FAX: +48 (0) 22 583 92 76
URL: www.dlink.pl

Hungary
R-k-czi-t 70-72
HU-1074
Budapest
Hungary
TEL : +36 (0) 1 461 30 00
FAX: +36 (0) 1 461 30 09
URL: www.dlink.hu

Singapore
1 International Business Park
#03-12 The Synergy
Singapore 609917
TEL: 65-6774-6233
FAX: 65-6774-6322
URL: www.dlink-intl.com

Australia
1 Giffnock Avenue
North Ryde, NSW 2113
Australia
TEL: 61-2-8899-1800
FAX: 61-2-8899-1868
URL: www.dlink.com.au

India
D-Link House, Kurla Bandra Complex Road
Off CST Road, Santacruz (East)
Mumbai - 400098
India
TEL: 91-022-26526696/56902210
FAX: 91-022-26528914
URL: www.dlink.co.in

Middle East (Dubai)
P.O.Box: 500376
Office: 103, Building:3
Dubai Internet City
Dubai, United Arab Emirates
Tel: +971-4-3916480
Fax: +971-4-3908881
URL: www.dlink-me.com

Turkey
Cetin Emec Bulvari, 74.sokak, ABC Plaza No:9/3
Ovecler/Ankara- TURKEY
TEL: 0090 312 473 40 55
FAX: 0090 312 473 40 58
URL: www.dlink.com.tr

Egypt
47,El Merghany street,Heliopolis
Cairo-Egypt
TEL: +202-2919035, +202-2919047
FAX: +202-2919051
URL: www.dlink-me.com

Israel
11 Hamanofim Street
Ackerstein Towers, Regus Business Center
P.O.B 2148, Hertzelia-Pituach 46120
Israel
TEL: +972-9-9715700
FAX: +972-9-9715601
URL: www.dlink.co.il

LatinAmerica
Isidora Goyeechea 2934
Ofcina 702
Las Condes
Santiago – Chile
TEL: 56-2-232-3185
FAX: 56-2-232-0923
URL: www.dlink.cl

Brazil
Av das Nacoes Unidas
11857 – 14- andar - cj 141/142
Brooklin Novo
Sao Paulo - SP - Brazil
CEP 04578-000 (Zip Code)
TEL: (55 11) 21859300
FAX: (55 11) 21859322
URL: www.dlinkbrasil.com.br

South Africa
Einstein Park II
Block B
102-106 Witch-Hazel Avenue
Highveld Technopark
Centurion
Gauteng
Republic of South Africa
TEL: 27-12-665-2165
FAX: 27-12-665-2186
URL: www.d-link.co.za

Russia
Grafsky per., 14, floor 6
Moscow
129626 Russia
TEL: 7-495-744-0099
FAX: 7-495-744-0099 #350
URL: www.dlink.ru

China
No.202,C1 Building, Huitong Office Park,
No. 71, Jianguo Road, Chaoyang District, Beijing
100025, China.
TEL +86-10-58635800
FAX: +86-10-58635799
URL: www.dlink.com.cn

Taiwan
No. 289 , Sinhu 3rd Rd., Neihu District ,
Taipei City 114 ,Taiwan
TEL: 886-2-6600-0123
FAX: 886-2-6600-1188
URL: www.dlinktw.com.tw